EnCase® Forensic

USER GUIDE

Version 8.07

GUIDANCE SOFTWARE

From beginning to endpoint.

May 11, 2018

CONTENTS

Introduction to EnCase Forensic 23

EnCase Forensic 23

CHAPTER 1 Installing and Configuring EnCase 25

Overview 27
Registering your Product 27
System Requirements 27
License Manager 32
Installation Overview 33
Installing EnCase Forensic Examiner 33
Installing License Manager 35
Activating an Electronic License 35
Creating a New Electronic Request File 35
Reactivating an Electronic License 36
If You Already Have a Security Key 36
Uninstalling EnCase 36
Reinstalling EnCase 37
Configuration Options 37
Global Options 37
Date Options 39
License Manager Options 40

Color Options 42
Font Options 42
Data Paths Options 43
Debug Options 44
Configuring Time Zone Settings 46
EnCase Folder Locations 47
Application Folder 47
User Data 48
User Application Data 49
Global Application Data 50
Install and Configure Evidence Processor Nodes 51
Checking the Windows Application Log 55

CHAPTER 2 Using Pathways to Streamline Workflows 57
Pathways Overview 59
Using a Pathway to Create a Full Investigation 59
Using a Pathway to Preview and Triage your Evidence 63
Custom Pathways 66
Creating a Custom Pathway 66
Modifying a Custom Pathway 68
Using Custom Pathway Headers 70

CHAPTER 3 Working with Cases 75
Overview 77
Launching EnCase 77
Using a Case Template to Create a Case 79
Case Options Settings 80
Case Templates 81
Adding Evidence to a Case 82
Setting Individual Case Options 84
Case Operations 85
Case Selections 85

Changing the Evidence Path if the Evidence File is Moved 86
Case Portability 87
Case Page Logo 88

CHAPTER 4 Case Backup 89
Overview 91
Case Backup Dashboard 91
Settings and Options 92
Automatic Backup 93
Backing up a New Case 93
Viewing Case Backup Options 94
Creating a Scheduled Backup 94
Creating a Custom Backup 94
Deleting a Backup 95
Changing Case Backup Settings 95
Specifying a Case File 96
Specifying a Backup Location 97
Restoring a Case from Backup 97

CHAPTER 5 Acquiring Devices and Evidence 101
Overview 103
Sources of Acquisitions 103
Canceling an Acquisition 104
Types of Evidence Files 104
EnCase Evidence Files 104
Logical Evidence Files 105
Raw Image Files 105
Single Files 106
Verifying Evidence Files 106
Acquiring a Local Drive 106
Acquiring Non-local Drives 107
Audit Drive Space 107

Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA) 107
Using a Write Blocker 108
Windows-based Acquisitions with Tableau and FastBloc Write Blockers 108
Acquiring in Windows using FastBloc SE 109
Acquiring in Windows without a Tableau or FastBloc Write Blocker 109
Acquiring a Disk Running in Direct ATA Mode 109
Acquiring Disk Configurations 110
Software RAID 110
RAID-10 111
Hardware Disk Configuration 111
Windows NT Software Disk Configurations 111
Support for EXT4 Linux Software RAID Arrays 112
Dynamic Disk 113
Disk Configuration Set Acquired as One Drive 113
Disk Configurations Acquired as Separate Drives 114
Acquiring Other Types of Supported Evidence Files 115
CD-DVD Inspector File Support 115
Acquiring a DriveSpace Volume 116
Reacquiring Evidence 116
Reacquiring Evidence Files 117
Retaining the GUID During Evidence Reacquisition 117
Adding Raw Image Files 117
Restoring a Drive 118

CHAPTER 6 Processing Evidence 121

Overview 123
Running Evidence Processor Options Incrementally 127
Conducting a Network Preview without a SAFE 129
Creating Direct Agents 129
Adding a Direct Network Preview Device 131
Evidence Processor Prioritization 133

Evidence Processor Settings 134
Recovering Folders 135
Analyzing Protected Files 135
Analyzing Hashes 136
Analyzing Entropy Values 136
Analyzing File Signatures 138
Expanding Compound Files 138
Finding Email 139
Finding Internet Artifacts 139
  Firefox Artifacts 140
  Safari Artifacts 141
Searching With Keywords 143
  Adding a New Keyword 145
  Creating a New Keyword List 147
  Searching for Keywords in Process Memory 147
Creating an Index 148
  Indexing Text in Slack and Unallocated Space 148
  Setting Word Delimiters for Indexing 150
  Add Word Delimiters to Search Index 150
  Selecting a Language Index 151
Creating Thumbnails 153
Running EnScript Modules 153
  System Info Parser 154
  File Carver 155
  Windows Event Log Parser 157
  Windows Artifact Parser 157
  Unix Login 158
  Linux Syslog Parser 158
  Macintosh OS X Artifacts Parser 158
Result Set Processing 162
  Processing a Result Set 162
  Launching Processor Options from the Results Tab 163
  Creating Result Sets in Entries and Artifacts Views 163

Overwriting the Evidence Cache 164
EnScript Application UI 165
Home Page 165
Case Page 166
Processor Manager 166
Processor Node Installation 167
Opening the Processor Manager 167
Adding Processor Nodes to the Processor Manager 167
Configuring Processor Nodes 168
Process Evidence Menu 170
Queuing Evidence for Processing 171
Processor Manager Tab 173
Processor Manager Toolbar 178
Running Multiple Instances of EnCase from the Same Machine 181
Processor Manager Error and Information Messages 181
Show Logging 190
Acquiring and Processing Live Previews 191
Live Previews of Local Devices 192
Direct Network Previews 192
Crossover Previews 192

CHAPTER 7 Browsing and Viewing Evidence 193
Overview 195
The EnCase Interface 195
Navigating the Tree Pane 197
Navigating the Table Pane 198
Adjusting Spacing in a Table 201
Viewing Content in the View Pane 202
Using Views/Tabs 208
Right Hamburger Menu 209
Changing Text Color 209
Navigating the Evidence Tab 210

Navigating the Artifacts Tab 215
Filtering Your Evidence 215
Running an Existing Filter 216
Creating a Filter 216
Editing a Filter 217
Deleting a Filter 217
Sharing Filters 217
Conditions 218
Running an Existing Condition 218
Creating a New Condition 219
Editing Conditions 222
Sharing Conditions 222
Printing a Condition 222
Browsing Through Evidence 223
Check for Evidence when Loading a Case 223
Finding the Location of an Evidence Item 223
Determining the Time Zone of Your Evidence 224
Viewing Related Items 226
Browsing Images 226
Viewing Evidence 227
Creating Custom File Types 227
Viewing Multiple Evidence Files Simultaneously 229
Viewing Multiple Artifacts Simultaneously 229
Viewing Contents of 7-Zip Files 229
Macintosh Artifacts 230
Displaying HFS+ File System Compressed Files 230
HFS+ Extended Attributes 230
HFS+ Directories Hard Links 231
Finder Data and .DS_Store 232
Displaying Permissions for HFS+ Files and Directories 233
Macintosh OS X Media Containers 234
Viewing Processed Evidence 236
Viewing Compound Files 236

Repairing and Recovering Inconsistent EDB Database Files 237
Viewing Email 238
Viewing Attachments 239
Showing Conversations 239
Displaying Related Messages 240
Showing Duplicate Email Messages in a Conversation 241
Exporting to *.msg 241

CHAPTER 8 Searching Through Evidence 243

Overview 245
Index Searches 245
Tag Searches 245
Keyword Searches through Raw Data 246
Viewing and Saving Search Results 246
Searching Indexed Data 246
Search Operators and Term Modifiers 249
Search Fields 255
Reserved Characters 256
Finding Tagged Items 257
Keyword Searching Through Raw Data 257
Refreshing Search Results during a Keyword Search 260
Retrieving Keyword Search Results 261
Bookmarking Keyword Search Results 262
Analyzing Individual Search Results 262
Viewing Saved Search Results 262
Creating a LEF from Search Results 264
Finding Data Using Signature Analysis 264
Adding and Modifying File Signature Associations 265
Running File Signature Analysis against Selected Files 267
Exporting Data for Additional Analysis 268
Copying Files 269
Copying Folders 271

Exporting Search Results for Review 272
Creating a Review Package 273
Analyzing and Tagging a Review Package 274
Exporting a Review Package 276
Importing a Review Package 276

CHAPTER 9 Hashing Evidence 279
Overview 281
Hashing Features 281
Working with Hash Libraries 282
Creating a Hash Library 282
Creating a Hash Set 283
Adding Hash Values to a Hash Set 284
Adding Results to a Hash Library 286
Querying a Hash Library 287
Adding Hash Libraries to a Case 288
Viewing Hash Sets Associated with an Entry 288
Managing Hash Sets and Hash Libraries Associated with a Case 290
Viewing and Deleting Individual Hash Items 290
Changing Categories and Tags for Multiple Hash Sets 290
Importing Hash Sets 291
NSRL Hash Sets 291
Integration with Project VIC 292

CHAPTER 10 Bookmarking Items 295
Overview 297
Working with Bookmark Types 297
Highlighted Data or Sweeping Bookmarks 297
Notable File Bookmarks 300
Bookmarking Case Analyzer Data 302
Table Bookmarks 304
Transcript Bookmarks 304

Notes Bookmarks ... 305
Bookmarking Pictures in Gallery View ... 306
Bookmarking a Document as an Image ... 307
Working with Bookmark Folders ... 307
Bookmarking Template Folders ... 307
Creating New Bookmark Folders ... 308
Editing Bookmark Folders ... 309
Deleting Bookmark Folders ... 309
Editing Bookmark Content ... 309
Editing Bookmarks ... 309
Renaming Bookmarks ... 310
Decoding Data ... 310
Quickly Viewing Decoded Data ... 311
Viewing Decoded Data by Type ... 311

CHAPTER 11 Tagging Items 315

Overview ... 317
Creating Tags ... 317
Tagging Items ... 319
Hot Keys for Tags ... 319
Viewing Tagged Items ... 320
Hiding Tags ... 321
Deleting Tags ... 321
Changing the Tag Order ... 322
Select Tagged Items ... 322

CHAPTER 12 Using EnCase Portable 323

Overview ... 325
Creating EnCase Portable Jobs ... 326
Creating Jobs ... 327
System Modules ... 334
Search Modules ... 338

Log Parser Modules 349
Collection Modules 351
Collecting Evidence 355
Running a Portable Job 355
Viewing Results to Triage Information 357
Copying Evidence 365
Analyzing and Reporting on Data 365
Selecting Target Databases 366
Creating a Report 366
Exporting a Report 373
Maintenance 374
Preparing Portable Devices 374
Modifying the EnCase Portable Device Configuration 375
Preparing Additional USB Storage Devices 377
Configuring EnCase Portable for NAS Licensing 378
Troubleshooting 379
FAQs 381

CHAPTER 13 Generating Reports 387

Overview 389
Bookmarking Data for Reports 389
Triage Report 390
Using Report Templates 397
Report Template Structure 398
Formatting Report Templates 399
Editing Report Templates to Include Bookmark Folders in Reports 405
Report Object Code (ROC) 413
Layout Elements 413
Content Display Elements 416
Report Template Wizard 420
Connecting Bookmark Folders and Report Sections 420
Hiding Empty Report Sections 423

Creating Hyperlinks to an Exported Item from Report Templates 424
Using Bookmarks to Link to an External File 424
Exporting a Report to Display Hyperlinks 426
Exporting a Metadata Report to Display Hyperlinks 426
Adding a Hyperlink to a URL 427
File Report EnScript 427
Running the File Report EnScript 428
Saving the File Report 429
Viewing a Report 429

CHAPTER 14 Acquiring Mobile Data 431
Overview 433
Installing the Mobile Driver Pack 433
Types of Data Acquisition 433
Data Parsing 434
Acquiring Data from Different Devices 434
Acquiring Mobile Device Data (General Process Description) 435
Acquisition via Automatic Device Detection 437
Acquisition via Manual Plug-in Selection 438
Acquiring Data from iPhones/iPods/iPads/iPod Touches 439
About Data Acquisition of iPhones/iPods/iPads/iPod Touches 439
Acquiring Data from Android OS Devices (Including Kindle Fire Tablets and Android Wear) 465
About Data Acquisition from Android OS Devices 465
Android Device Rooting 466
Android OS Devices 467
LG Devices with Android OS 4.4.2 - 5.1.1 480
Samsung Devices with Android OS 4.4.4 – 6.0.1 483
Android Spreadtrum Devices 485
Acquiring Data from Tizen Devices 486
Preparing Device for Acquisition- Tizen 487
Data Acquisition- Tizen 487

Acquired Data- Tizen 487
Supported Models - Tizen 488
Tizen Devices FAQ 488
Acquiring Data from RIM BlackBerry Devices 488
Data Acquisition - BlackBerry 488
Acquired Data - BlackBerry 489
Supported Models - BlackBerry 490
RIM BlackBerry FAQ 490
Acquiring Data from Symbian OS Smartphones 491
About Data Acquisition from Symbian OS Smartphones 491
Data Acquisition - Nokia Symbian 509
Acquired Data - Nokia Symbian 509
Supported Models - Nokia Symbian 509
Nokia Symbian OS Physical Acquisition FAQ 509
Acquiring Data from a WebOS Based Device 510
Preparing Device for Acquisition - WebOS 510
Data Acquisition - WebOS 512
Acquired Data - WebOS 512
Supported Models - WebOS 512
WebOS Devices FAQ 513
Acquiring Data from PDAs 513
About Data Acquisition from PDA 513
Psion 16/32-bit Devices FAQ 517
Palm OS Devices FAQ 520
Acquiring Data from GPS Devices 534
Acquiring Data from Feature Phones 547
About Feature Phone Plug-ins 547
Acquiring Data from SIM Cards 584
Data Acquisition - SIM Cards 584
Acquired Data - SIM Cards 584
Supported Models (Card Readers) - SIM Cards 586
SIM Card Reader FAQ 588

Acquiring Data from Memory Cards/Mass Storages/e-Readers/Portable Devices 589
Importing Data 592
Importing Data from Cellebrite UFED Cases 592
Importing Data from iOS Backup Files 593
Importing Data from RIM BlackBerry 1.x - 7.x Backup Files 595
Importing Data from RIM BlackBerry 10.x Encrypted Backup Files 596
Importing GPS and KML Files 597
Importing Tarantula Data 598
Importing Cloud Data 598
Extracting Authentication Data File 599
Importing Cloud Data 599
Imported Cloud Data 601
Cloud Data Importing FAQ 602
General Acquisition FAQ 602

CHAPTER 15 Working with Non-English Languages 609
Overview 611
Configuring EnCase to Display Non-English Characters 611
Changing the Default Code Page 612
Setting the Date Format 613
Assigning a Unicode Font 613
Viewing Unicode Files 614
Text Styles 615
Configuring Windows for Additional Languages 615
Configuring the Keyboard for Additional Languages 615
Entering Non-English Content with the Windows Character Map 616

CHAPTER 16 Using LinEn 619
Overview 621
Creating a LinEn Boot Disk 621
Configuring Your Linux Distribution 622

Obtaining a Linux Distribution ... 622
LinEn Setup Under SUSE ... 622
LinEn Setup Under Red Hat ... 623
Performing Acquisitions with LinEn ... 623
Setup for a Drive-to-Drive Acquisition ... 624
Drive-to-Drive Acquisition ... 625
LinEn Evidence Verification ... 632
Window Menu ... 636
Console Window ... 636
Thread Monitor Window ... 637
Edit Menu ... 638
LinEn Command Line ... 640
Crossover Cable Preview or Acquisition ... 645
LinEn Manual Page ... 646

CHAPTER 17 EnCase Decryption Suite 649

Overview ... 652
Disk and Volume Encryption ... 652
Supported Encryption Products ... 653
EDS Commands and Tabs ... 655
Analyze EFS ... 655
Secure Storage Tab ... 656
Passware Integration ... 659
Safeboot Encryption Support ... 660
Check Point Full Disk Encryption Support (Volume Encryption) ... 663
Username and Password Authentication ... 663
Challenge-Response Authentication ... 665
BitLocker Encryption Support (Volume Encryption) ... 667
Recovery Key and Recovery Password Files ... 667
Decrypting a BitLocker Encrypted Device Using Recovery Key ... 668
Decrypting a BitLocker Encrypted Device Using Recovery Password ... 670
Full Volume Encryption (FVE) AutoUnlock Mechanism ... 671

Physical RAID Encryption Support 672
Successful BitLocker Decryption 673
Unsuccessful BitLocker Decryption 674
Saved BitLocker Credentials in Secure Storage 675
WinMagic SecureDoc Encryption Support 675
WinMagic SecureDoc Self Encrypting Drive (SED) Support 677
GuardianEdge Encryption Support 678
Supported GuardianEdge Encryption Algorithms 678
GuardianEdge Hard Disk and Symantec Endpoint Encryption Support 679
Symantec Endpoint Encryption Support 681
Symantec Endpoint Encryption v11.1.1 support 681
Sophos SafeGuard Support 682
Decrypting a Disk 682
Decrypting Sophos SGN-Encrypted Evidence Using a Challenge/Response Session in EnCase 682
Obtaining Response Codes from the Sophos SGN Website 683
Completing the Challenge/Response Session 684
Utimaco SafeGuard Easy Encryption Support 685
Supported Utimaco SafeGuard Easy Encryption Algorithms 685
Utimaco Challenge/Response Support 685
Utimaco SafeGuard Easy Encryption Known Limitation 688
PGP Whole Disk Encryption (WDE) Support 689
Obtaining Whole Disk Recovery Token Information 689
Obtaining Additional Decryption Key (ADK) Information 690
PGP Decryption using the Passphrase 690
Dell Data Protection Enterprise (formerly Credant Mobile Guardian) Encryption Support 691
Enabling an Examiner Machine to Identify and Decrypt Credant Files 691
Decrypting Credant Files Accessible on the Network 691
Decrypting Offline Dell Data Protection Enterprise/Credant Mobile Guardian Files 692
Decrypting Credant Files on Microsoft EFS 694
McAfee Endpoint Encryption Support 694

S/MIME Encryption Support 695
Troubleshooting a Failed S/MIME Decryption 696
NSF Encryption Support 696
Recovering NSF Passwords 696
Lotus Notes Local Encryption Support 697
Determining Local Mailbox Encryption 697
Parsing a Locally Encrypted Mailbox 697
Encrypted Block 698
Decrypted Block 698
Locally Encrypted NSF Parsing Results 699
Windows Rights Management Services (RMS) Support 700
RMS Decryption at the Volume Level 700
RMS Decryption at the File Level 701
RMS Protected Email in PST 701
Windows Key Architecture 701
Dictionary Attacks 702
Built-In Attacks 703

CHAPTER 18 Using the EnScript Programming Language 707
Overview 709
The EnScript Language 709
App Central 709
EnScript Launcher 709

CHAPTER 19 Virtual File System 711
Overview 713
Evidence File Formats Supported by VFS 713
Mounting Evidence with VFS 713
Mounting a Single Drive, Device, Volume, or Folder 713
Mount Network Share Options 714
Compound Files 715
Encrypting File System 715

RAIDs ... 717
Deleted Files ... 718
Internal Files and File System Files ... 718
RAM and Disk Slack ... 718
Other File Systems ... 719
ext2, ext3, UFS, and Other File Systems ... 720
Dismounting the Network Share ... 721
Changing the Mount Point ... 721
Accessing the Share ... 721
Using the EnCase VFS Name Column ... 721
Using Windows Explorer with VFS ... 722
Third Party Tools ... 722
Malware Scanning with VFS ... 722
Other Tools and Viewers ... 723
Temporary Files Reminder ... 724
VFS Server ... 724
Configuring the VFS Server ... 725
Restrict Access by IP Address ... 726
Connecting the Clients ... 727
Closing the Connection ... 727
Troubleshooting the Virtual File System ... 728

CHAPTER 20 Physical Disk Emulator 729
Overview ... 731
Evidence File Formats Supported by EnCase PDE ... 731
Using Physical Disk Emulator ... 731
Starting Physical Disk Emulator ... 731
Configuring the PDE Client ... 732
Mounting Non-Windows Devices ... 733
Accessing the Local Disk in Windows Explorer ... 733
Saving and Dismounting the Emulated Disk ... 733
Closing and Changing the Emulated Disk ... 735

Temporary Files Redirection 735
Third Party Tools 735
Using Third Party Tools 736
Boot Evidence Files and Live Systems with VMware 736
Initial Preparation 736
New Virtual Machine Wizard 737
Booting the Virtual Machine 738
VMware/EnCase PDE FAQs 739
PDE Troubleshooting 740

CHAPTER 21 FastBloc SE 743
Overview 745
Write Blocking and Write Protecting a Device 745
Write Blocking a USB, FireWire, or SCSI Device 745
Write Protecting a USB, FireWire, or SCSI Device 746
Removing Write Block from a USB, FireWire, or SCSI Device 746
Disk Caching and Flushing the Cache 747
Troubleshooting 747

CHAPTER 22 Support 751
Overview 753
Find Support Online 753
Access the Customer Community 754
Browse the Knowledge Base 755
Log and Track Issues 755
Register your Product 755
Register your Account 755
Contact Guidance Software 756
Contact Sales 756
Contact Customer Service 756
Contact Technical Support 756
Contact EnCase eDiscovery Review Technical Support 757

Index 759

INTRODUCTION TO ENCASE FORENSIC

EnCase Forensic enables you to collect forensically sound data and conduct complex large scale investigations from beginning to end.

EnCase Forensic is designed to be used by:

- Those responsible for collecting evidence
- Forensic examiners and analysts
- Forensic examiners who develop and use EnScript code to automate repetitive or complex tasks

With EnCase Forensic these types of investigators can:

- Acquire data in a forensically sound manner using software with an unparalleled record in courts worldwide
- Investigate and analyze data from multiple platforms—Windows, Linux, AIX, OS X, Solaris, and more—using a single tool
- Find information despite efforts to hide, cloak, or delete
- Easily manage large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space
- Create exact duplicates of original data, verified by hash and Cyclic Redundancy Check (CRC) values
- Transfer evidence files directly to law enforcement or legal representatives
- Review options that allow non-investigators, such as attorneys, to review evidence with ease
- Use reporting options for quick report preparation

EnCase Forensic

EnCase Forensic enables you to collect forensically sound data and conduct complex large scale investigations from beginning to end.

EnCase Forensic is designed to be used by:

- Those responsible for collecting evidence
- Forensic examiners and analysts
- Forensic examiners who develop and use EnScript code to automate repetitive or complex tasks

With EnCase Forensic these types of investigators can:

- Acquire data in a forensically sound manner using software with an unparalleled record in courts worldwide
- Investigate and analyze data from multiple platforms—Windows, Linux, AIX, OS X, Solaris, and more—using a single tool
- Find information despite efforts to hide, cloak, or delete
- Easily manage large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space
- Create exact duplicates of original data, verified by hash and Cyclic Redundancy Check (CRC) values
- Transfer evidence files directly to law enforcement or legal representatives
- Review options that allow non-investigators, such as attorneys, to review evidence with ease
- Use reporting options for quick report preparation

CHAPTER 1

INSTALLING AND CONFIGURING ENCASE

Overview	27
Registering your Product	27
System Requirements	27
License Manager	32
Installation Overview	33
Installing EnCase Forensic Examiner	33
Installing License Manager	35
Activating an Electronic License	35
Uninstalling EnCase	36
Reinstalling EnCase	37
Configuration Options	37
Configuring Time Zone Settings	46
EnCase Folder Locations	47
Install and Configure Evidence Processor Nodes	51

Overview

This chapter describes the process of installing EnCase Forensic and related components.

This chapter lists the default locations of installation directories and files and also provides information about configuring EnCase settings.

Registering your Product

When you receive your product, you must register it with Guidance Software to receive updates.

System Requirements

Before you begin, make sure you have:

- An EnCase security key (dongle), or an electronic license and connection information
- An optional certificate file for users who want to activate an EnCase Version 6 dongle to run EnCase Version 8
- Installation files for the current release of EnCase

SUPPORTED OPERATING SYSTEMS

- Microsoft Windows 7 SP1 through Windows 10
- Microsoft Windows Server through Version 2016

MINIMUM SUGGESTED SYSTEM REQUIREMENTS FOR EXAMINATION MACHINES

- 4 core processor or better
- 16 GB RAM or better
- 200 GB or larger Solid State Drive (SSD) for Case Data
- 200 GB or larger Solid State Drive (SSD) for Evidence Cache Data
- 1 TB or larger Hard Disk Drive (HDD) for Evidence Data

MINIMUM SUGGESTED SYSTEM REQUIREMENTS FOR MACHINES RUNNING THE SAFE

- 2 core processor
- 4 GB RAM
- 40 GB Spindle or SSD

RECOMMENDATIONS FOR SPECIFIC WORKLOADS

For best performance based on specific workloads, examination computers should meet or exceed the following hardware and software requirements:

Basic Recommended System Requirements (for small workloads)	
Operating System	Windows 8.1 64-bit
CPU	Core i5
Memory	16 GB (Four 4 GB Modules)
Network	Gigabit network card
OS Drive	120 GB SSD
Evidence Storage Drive	1 TB SSD
Evidence Backup Drive	Two or three 2 TB hard drives
I/O Interfaces	USB 3.0, eSATA, SATA, SATA 3
Flash Media Readers	Multi-reader
Optical Drive	Blu-Ray R/W
Display	Single 21”, 22”, 23” or 24” LCD
RAID Card	N/A
Uninterruptible Power Supply	650 VA
Write Blocker	TD2u

Recommended System Requirements (for best single-caseload performance)	
Operating System	Windows 8.1 64-bit Windows Server 2012 R2 64-bit

Recommended System Requirements (for best single-caseload performance)	
CPU	Core i7
Memory	64 GB (Eight 8 GB Memory Modules)
Network	Gigabit network card
OS Drive	256 GB SSD
Evidence Storage Drive	4x 512 GB SSD in RAID 10 configuration
Evidence Backup Drive	RAID of several 4 TB hard drives
I/O Interfaces	Thunderbolt, USB 3.0, eSATA, SATA, SATA 3
Flash Media Readers	Multi-reader
Optical Drive	Blu-Ray R/W
Display	Dual 24”+ LCD
RAID Card	N/A
Uninterruptible Power Supply	1000 VA
Write Blocker	TD2u

Recommended System Requirements (equipped to handle larger simultaneous workloads)	
Operating System	Windows 8.1 64-bit Windows Server 2012 R2 64-bit
CPU	Dual processor core i7 or Xeon E7 family
Memory	128 GB (Eight 16 GB Memory Modules)
Network	10 gigabit network card
OS Drive	256 GB SSD
Evidence Storage Drive	Multi-TB RAID 10

Recommended System Requirements (equipped to handle larger simultaneous workloads)	
Evidence Backup Drive	Fiber channel SAN
I/O Interfaces	Thunderbolt, USB 3.0, eSATA, SATA, SATA 3
Flash Media Readers	Multi-reader
Optical Drive	Blu-Ray R/W
Display	Multiple 27”+ LCD
RAID Card	N/A
SAS Card	N/A
Uninterruptible Power Supply	1000 VA
Write Blocker	TD2u

Recommended System Requirements for Application Server System (optimal solution for multiple simultaneous and frequent exceptionally large workloads)	
Operating System	Windows Server 2012 R2 64-bit
CPU	Dual CPU E7 family
Memory	128 GB (Eight 16 GB Memory Modules)
Network	10 Gigabit network card
OS Drive	256 GB SSD
Evidence Storage Drive	Multi-TB RAID 10
Page File Drive	Separate 256 GB SSD

Recommended System Requirements for Application Server System (optimal solution for multiple simultaneous and frequent exceptionally large workloads)	
Evidence Backup Drive	Fiber channel SAN
I/O Interfaces	Thunderbolt, USB 3.0, eSATA, SAS
Flash Media Readers	Multi-reader
Optical Drive	Blu-Ray R/W
Display	Multiple 27"+ LCD
RAID Card	N/A
SAS Card	N/A
Uninterruptible Power Supply	1500 VA
Write Blocker	TD2u

Recommended System Requirements for Basic 'Field' Laptop	
Operating System	Windows 8.1 64-bit
CPU	Core i5 M
Memory	8 GB
Network	Gigabit network card
Hard Drive	256 GB SSD
Evidence Storage Drive	1 TB SSD
I/O Interfaces	USB 3.0, eSATA
Optical Drive	Blu-Ray R/W
Write Blocker	TD2u

Recommended System Requirements for a High Performance 'Field' Laptop	
Operating System	Windows 8.1 64-bit
CPU	Core i7 desktop
Memory	32 GB
Network	Gigabit network card
OS Drive	512 GB SSD
Evidence Storage Drive	Synology Diskstation
I/O Interfaces	Thunderbolt, USB 3.0, eSATA
Optical Drive	Blu-Ray R/W
Battery	High capacity spare battery
Write Blocker	TD2u

License Manager

The License Manager acts as a software license repository and server. The License Manager (previously referred to as "NAS") provides license management services for most Guidance Software products. In addition to being delivered by License Manager, licenses can also be delivered by physical security key (dongle) or as a software license tied directly to the workstation. The License Manager is a standalone application that can be installed at the same time as the SAFE or independently depending on your preference.

By distributing licenses to users across a network, License Manager simplifies license management by eliminating the need to distribute physical security keys (dongles) to individual computers. License Manager is typically used in laboratory environments with multiple examiners and multiple copies of EnCase Forensic.

When you run EnCase on a computer, it first searches for a physical security key or local software license for licensing information unless network-based licensing is enabled. To enable an Examiner computer to use software licensing through License Manager, you must first install License Manager and configure Examiner machines. Once configured, individual workstation access to License Manager can easily be enabled or disabled within the EnCase

application. See the *Guidance Software SAFE User Guide* for installation and configuration instructions. If no valid security key or software license is found, EnCase opens in Acquisition mode.

For more information about implementing or managing the License Manager and the SAFE, see the *Guidance Software SAFE User Guide*.

Installation Overview

The EnCase Forensic Examiner is the primary application used to conduct investigations. Other components provide additional functionality.

Select the installation option that matches how you intend to use EnCase Forensic:

- If you plan on deploying EnCase Forensic on one or more examiner machines and intend to manually install and manage physical security keys (dongles) or software licenses for each machine, use the standalone installer for EnCase Forensic for individual examiner machines. See Installing EnCase Forensic Examiner below.
- If you plan on using EnCase Forensic on multiple machines and want to centralize EnCase licensing, you must install License Manager on a machine on your network to hold and serve your software licenses. You can install License Manager on a dedicated machine, or on an examiner machine. Physical security keys and machine-specific electronic licenses can be used in conjunction with software licenses served by License Manager.
    - To install EnCase Forensic Examiner on individual machines, see Installing EnCase Forensic Examiner below.
    - To install License Manager on a machine on your network, see Installing the SAFE and License Manager in the *Guidance Software SAFE User Guide*.

Installing EnCase Forensic Examiner

To install EnCase on an individual examiner machine:

1. Open the EnCase Examiner installation file. If you have a security key, do not insert it until after installation is complete.
2. Accept the default installation path (`C:\Program Files\EnCase8`), or enter your own installation path and click **Next**.
    - If you used the same directory for a previous installation of EnCase, the installer overwrites any existing program files, logs, and drivers.

3. The EnCase License Agreement displays. Read it and click the **I Agree and accept** check-box. Click **Next**.

4. The installation path displays. Depending on your installation history, the following check-box options display:
   - **Install HASP Drivers** installs the latest version of the HASP security key (dongle) drivers. Guidance Software recommends selecting this checkbox if you are upgrading from a previous version of EnCase, or if you are working in an environment using a mix of both Sentinel/Aladdin HASP drivers and Codemeter security keys. This checkbox displays and is checked by default if you do not have HASP drivers installed. If you are reinstalling and have already installed the HASP drivers and the checkbox is present, leave the box unchecked.
   - The **Install CodeMeter Drivers** checkbox displays and is checked if you do not have a previous version of EnCase installed. Guidance Software recommends installing CodeMeter drivers.
   - **Reinstall CodeMeter Drivers** and **Reinstall HASP Drivers** may display if the installer detects you have previous versions of the drivers installed. CodeMeter drivers are always reinstalled. HASP drivers can be reinstalled if desired.

5. Click **Next**. Installation begins.
6. Click **Finish**. When the installation wizard has finished copying and installing EnCase, select **Reboot Now** to complete the installation immediately, or **Reboot Later**. To ensure the registration of installed DLL files and enable the drivers, you must reboot before running the application.
7. After the computer reboots, insert the security key into a USB port on your computer. With the program successfully installed, the shortcut to EnCase displays on your Desktop. If you are using a CodeMeter security key, the CodeMeter icon in the Windows system tray turns blue. You are now ready to use the product.

All EnCase users must have administrator permissions to view local devices on Windows computers running Vista operating systems and above.

To run EnCase as an administrator:

1. Right click the EnCase icon and click **Run as Administrator**.
2. Windows displays a prompt with the heading **An unidentified program wants access to your computer**.
3. Click **Allow**.

Installing License Manager

License Manager is an application is used to manage and serve electronic licenses for EnCase Forensic. You can install License Manager on a dedicated server or an examiner machine on your network.

Forensic users should use the stand-alone License Manager installer. While a SAFE and License Manager combined installer is available, the SAFE is no longer needed for Forensic users and need not be installed. For installation instructions, see Installing the SAFE and License Manager in the *Guidance Software SAFE User Guide*.

Activating an Electronic License

To activate your EnCase license electronically:

1. Open EnCase Forensic. Click on the question mark icon on the right side of the top menu bar. Select **Activate Electronic License** from the drop-down menu.

   Note: If you already have an active electronic license installed, a message displays. Click **OK** to remove the active current license, or **Cancel** to retain it.

2. The Activate Electronic License dialog displays. Enter the license key number you obtained via email from Guidance Software and your email address in the boxes provided.
3. Click **Next**. A second Activate Electronic License dialog displays.
   - Return to your **MyAccount** email and click the **Submit your file** link.
   - In the web page that displays, browse to the location of the License Request file, then click **Submit**.
   - Wait to receive an email response from **MyAccount**. In the License Activation portion of the email, click the link to save your License Activation file, then copy this file into the same folder as the License Request file.
4. Click **Next**. A third Activate Electronic License dialog displays.
5. Click **Finish** to complete the activation process.

Creating a New Electronic Request File

You can create a new electronic request file if you previously entered incorrect information.

To create a new electronic request file:

1. On the EnCase Home page, click the question mark in the upper right corner, then click **Activate Electronic License**. The Activate Electronic License dialog displays.

2. Click **Back**. In the dialog that displays, make the corrections to the license key number or the email address, then click **Next**.
3. Follow the steps in Activating an Electronic License on the previous page

Reactivating an Electronic License

If you already have an active license installed and you click **Activate Electronic License**, a message displays saying there is an active license installed and that if you want to install a new license, you must remove the current one.

Click **OK** to remove the active license or **Cancel** to retain the current active license.

If You Already Have a Security Key

If you already have a physical security key (dongle), and you purchase another copy of EnCase with an electronic license, the electronic license is fixed to the machine where it is installed. It cannot be moved to another computer. The security key can be moved from one machine to another.

Uninstalling EnCase

The EnCase uninstaller removes the corresponding version of EnCase from your computer.

To uninstall EnCase:

1. Make backups of evidence and case files prior to making modifications to any software on an examination machine.
2. Close any open versions of EnCase.
3. Open the Windows Control Panel and click **Uninstall a Program** under Programs.
4. Select the EnCase version to remove and click **Uninstall/Change**.
5. The EnCase uninstall wizard runs and the first screen displays.
6. Enter or navigate to the installation location in the Install Path field. The default for the current version is `C:\Program Files\Encase8`.
7. Click **Next**.
8. Select **Uninstall** and click **Next**. A progress bar displays during the uninstall process.
9. The last page of the uninstall wizard displays. Select **Reboot Later** or **Reboot Now** and click **Finish**. A reboot completes the uninstallation process.

Reinstalling EnCase

Use the EnCase Installation Wizard to reinstall EnCase. Reinstallation creates a new log file and reinstalls the following items:

- Application files
- Registry keys
- Needed user files
- Default configuration files

Note: Any modified EnScript files are overwritten during reinstallation. If you want to keep modified EnScript files, move them to another folder prior to reinstallation.

Reinstalling does not change:

- Licenses
- Certificates
- User settings

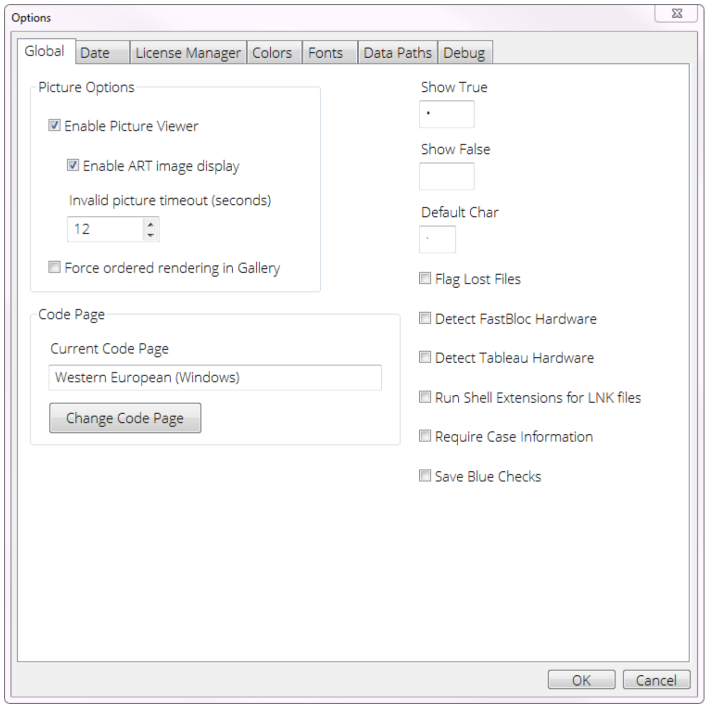
When reinstalling EnCase, make sure that your security key is inserted. If support on the security key has expired, a warning message displays.

Configuration Options

You can configure options for EnCase according to your needs or preferences, using the Configuration Options tabbed dialog. Each tab allows you to select a panel that controls a group of options, described in the following sections. To access the Configuration Options, select **Options** from the **Home** tab.

Global Options

The **Global** tab contains settings that apply to all cases.



In the Picture Options box, **Enable Picture Viewer** allows graphics to be displayed in various views.

Enable ART Image Display determines whether to display legacy ART image files. When EnCase Forensic encounters corrupt ART image files, application problems can occur. Enabling this setting minimizes the impact of corrupted ART files.

> **Note:** Rendering of ART files depends on the version of Internet Explorer installed. Current versions of Internet Explorer do not support ART files. If your version of Internet Explorer does not support ART files, EnCase cannot render them.

Invalid Picture Timeout (seconds) indicates the amount of time EnCase attempts to read a corrupt image file before timing out. After a timeout occurs, the corrupt file is sent to the cache and no attempt is made to re-read it.

Force ordered rendering in Gallery forces images to display in order, from left to right, sequentially by row. If you leave this box unchecked, images display in a gallery view as they become available. Although images display in order, the former view takes longer to complete, whereas images that display when rendering is not forced but not in order display more rapidly.

In the Code Page box, **Change Code Page** lets you change the default value of the code page from Western European (Windows) to another available code page. Set the global code page to display foreign language characters correctly.

Show True indicates a value of true in table columns displayed in the **Table** tab of the Table pane. The default indicator is a bullet, which you can change to a different character.

Show False indicates a value of false in table columns displayed in the **Table** tab of the Table pane. The default indicator is a blank space, which you can change to a different character.

Default Char specifies the character that EnCase uses on its displays to indicate that a box or cell is checked.

Flag Lost Files specifies whether the disk map shows lost clusters. Lost clusters are clusters that EnCase cannot determine as being used even though the file system indicates them as being used.

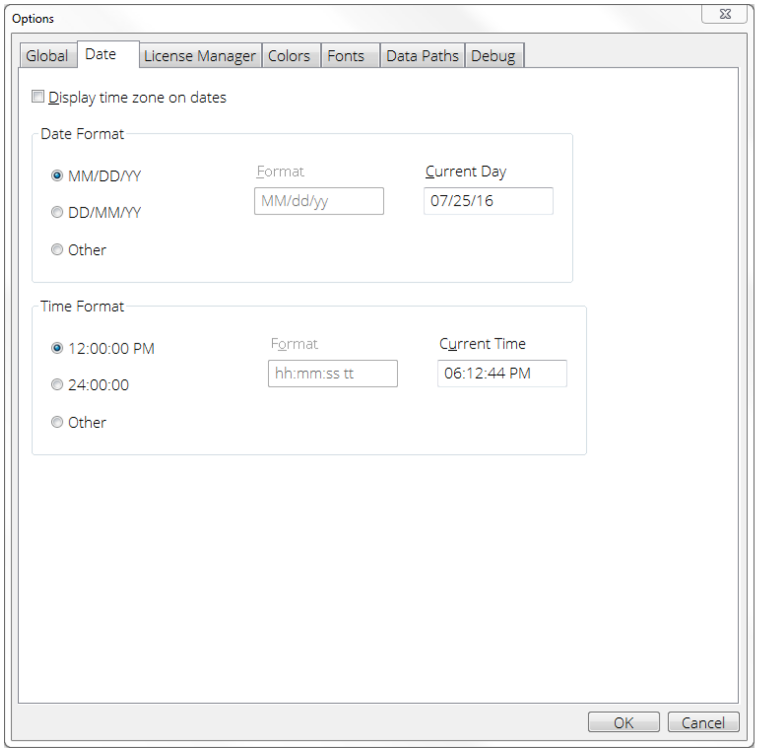
Detect FastBloc Hardware determines whether to search for legacy FastBloc hardware write blockers.

Detect Tableau Hardware determines whether to search for Tableau write blockers.

Run Shell Extensions for LNK Files enables EnCase to extract more data from .lnk files, which displays as IDList Data in the **Report** tab. Be aware that this option extracts LNK data locally, not from the acquired evidence. If you want to use this option on evidence data, you must run EnCase on the machine that contains the LNK files of interest.

Date Options

Customize date/time information associated with a case using the **Date** tab in Options.



Display time zone on dates includes the time zone in date/time columns.

Date Format includes these options:

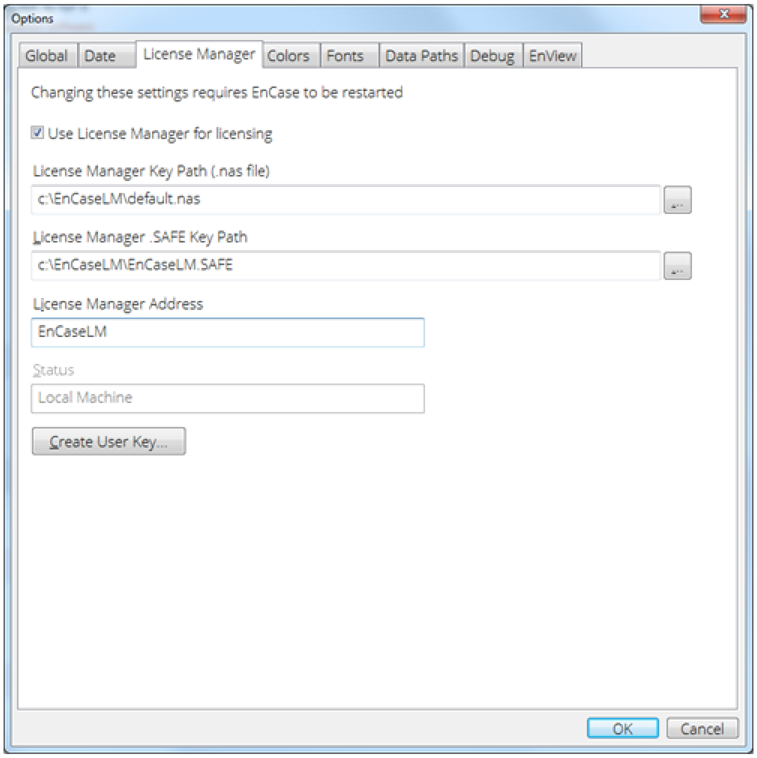
- **MM/DD/YY** (07/25/18)
- **DD/MM/YY** (25/07/18)
- **Other** lets you specify your own date format.
- **Current Day** displays the current date in the specified date format.

Time Format includes these options:

- **12:00:00 PM** uses a 12 hour clock for the time format.
- **24:00:00** uses a 24 hour clock for the time format.
- **Other** lets you specify your own time format.
- **Current Time** displays the current time in the specified time format.

License Manager Options

The options on the **License Manager** tab configure EnCase to receive software licensing information from License Manager instead of from a dongle inserted into the machine.



Use License Manager for licensing: Check this box to indicate use of License Manager to run the copy of EnCase on your computer.

License Manager Key Path: Specifies the full path of the user's licensing file. The license file for general licensing of EnCase is `default.nas`.

License Manager .SAFE Key Path: Enter the full path of the location of the EnCase SAFE public key file. This SAFE token file has a file signature of .SAFE and is found on the License Manager.

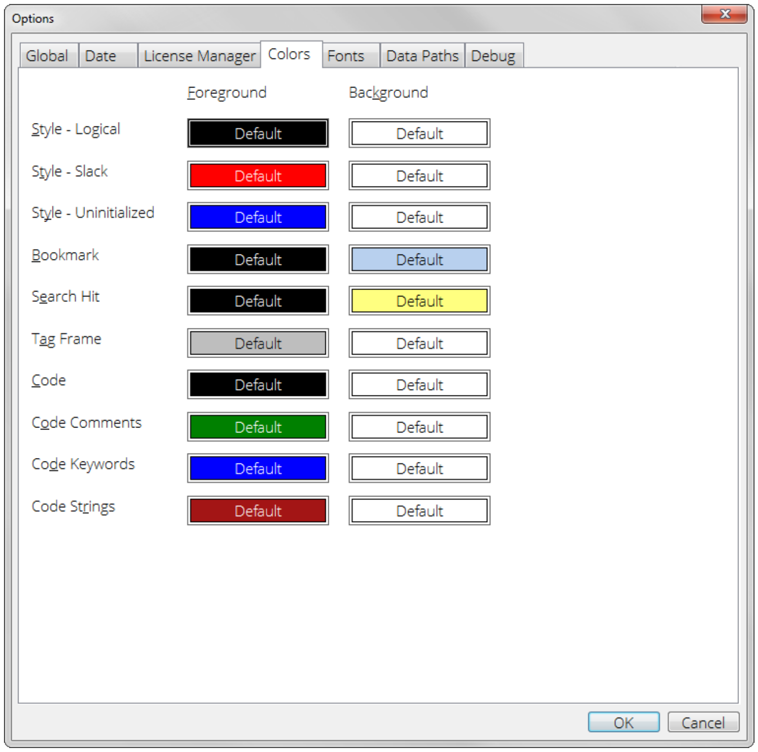
License Manager Address: Enter the IP address or machine name of the computer running the License Manager. If you are using a port other than 4446, precede the port number with the computer's IP address (for example, 192.168.1.34:4446).

Status: Displays the name or IP address of the computer on which the EnCase licensing files currently reside.

Create User Key...: Opens the Create User Key dialog. Do not use this button unless you are creating separate licenses for each computer belonging to your License Manager setup. For more information about using individual licenses, see the *Guidance Software SAFE User Guide*.

Color Options

Use the **Colors** tab to change the default colors associated with various case elements. This dialog shows the current foreground and background colors for the case element.



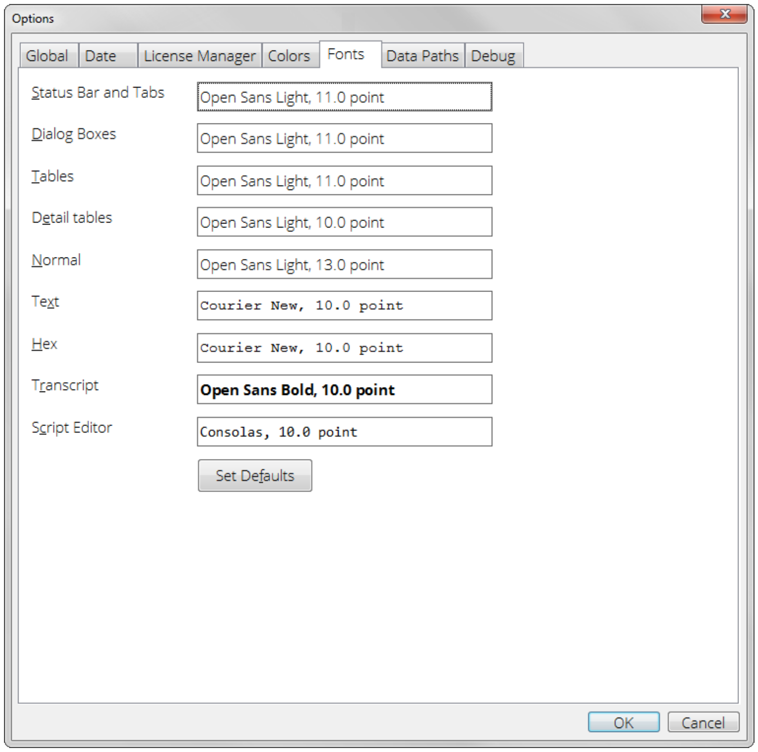
To change the colors for a listed EnCase element:

1. Double click the **Foreground** or **Background** associated with an element.
2. Click a box in the **Color** dialog to select that color.
3. Click **Define Custom Colors** to select from a larger palette of colors.
4. Click **OK** to accept the color change or **Cancel** to revert to the previous color.

> **Note:** Choice of color applies to the cell in the table. It does not affect the color of the font.

Font Options

Use the **Fonts** tab to customize the fonts used for EnCase user interface items, and in data panels and reports.



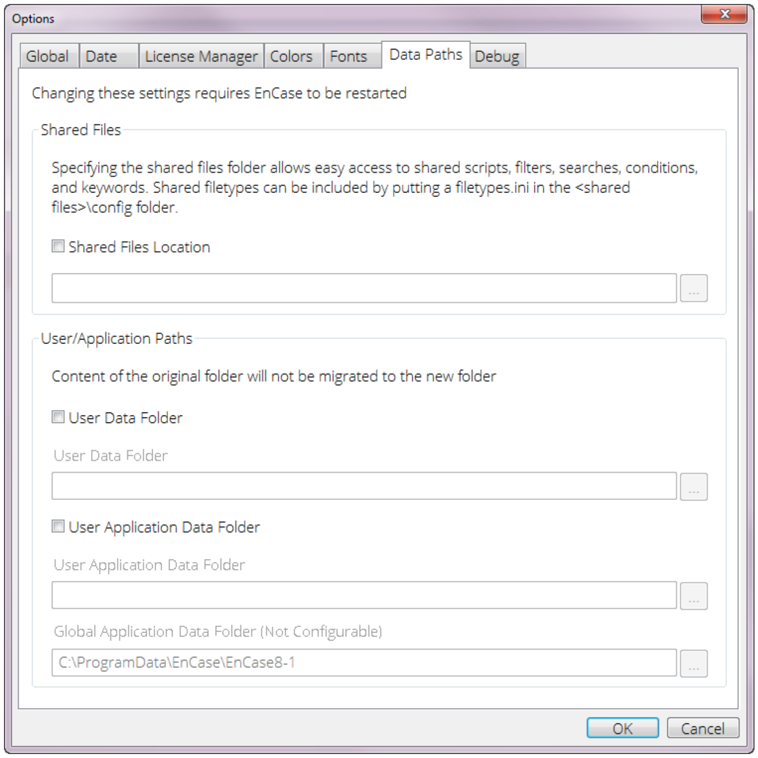
To customize the font for an element:

1. Double click the box associated with an item.
2. In the Font dialog, select your options and click **OK**. The text box previews the current font options.

> **Note:** If you change font settings and want to revert to the original settings, click **Set Defaults**.

Data Paths Options

Use the **Data Paths** tab to specify a path to a folder containing files that require shared access.

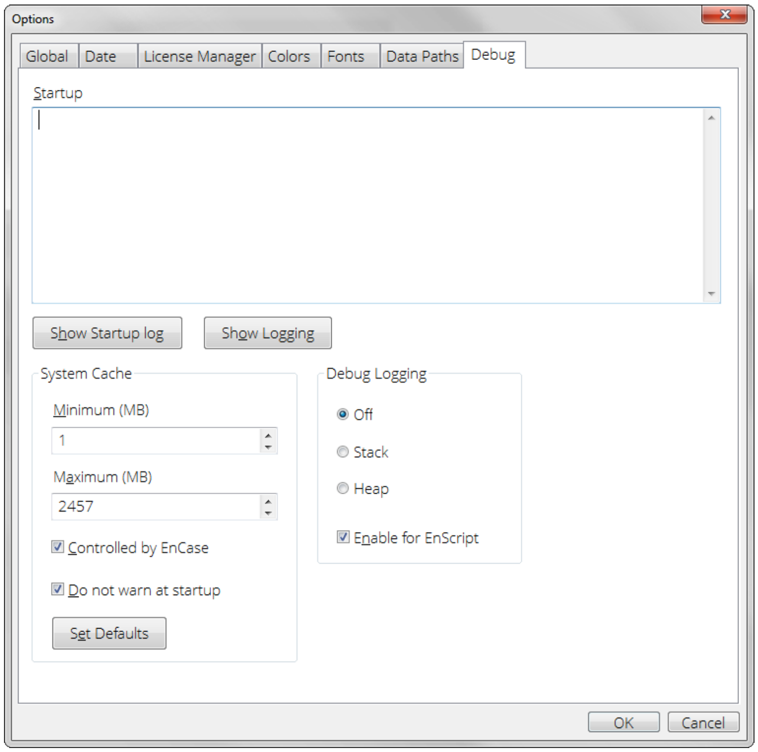


Specifying the shared files folder allows easy access to:

- Shared scripts
- Filters
- Searches
- Conditions
- Keywords

Debug Options

Use the **Debug** tab to specify debugging information and options.



The Startup panel displays operating system, application, and session information about your computer and about EnCase.

If the pane is empty, click **Show Startup Log** to display the information. The information is useful for troubleshooting purposes.

System Cache specifies the amount of physical memory for caching reads and writes of files on disk. The default value is 20 percent of the computer's physical memory (RAM).

- **Minimum (MB)**: The minimum size of the system cache in Megabytes; the default value is 1.
- **Maximum (MB)**: The maximum size of the system cache in Megabytes. The default value depends on the amount of physical memory available on the computer. You can manually set this value up to the maximum amount of physical memory available (although this is not recommended).
- **Controlled by EnCase**: Clicking this box allows EnCase to control the size of the system cache (recommended).
- **Do not warn at startup**: If you check this box, EnCase will not display warning messages when possible system memory issues occur.
- **Set Defaults:** Click this button to reset the system cache values to their default values.

Debug Logging allows you to select which logging action to take in the event of a crash:

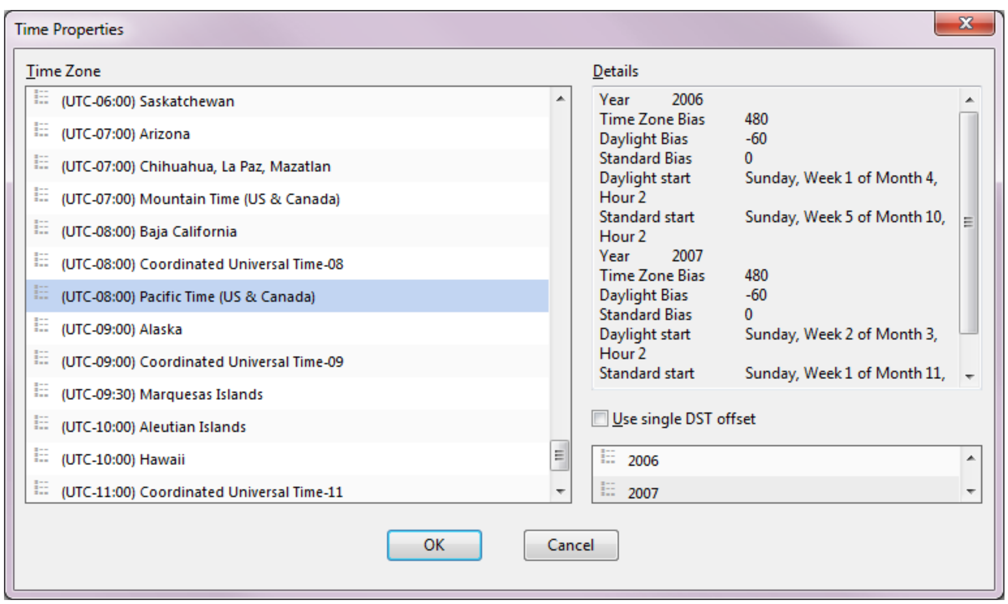
- **Off**: No debug logging is performed (default).
- **Stack**: This option saves a stack dump if EnCase crashes. This file contains data that the crashing subsystem used, the system DLLs loaded at the time of the event, and the version of EnCase. In most cases, the information written to the Stack dump log does not contain case specific data.
- **Heap**: This option saves a heap dump if EnCase crashes. It is the recommended option for most EnCase crash issues. The heap contains data from process memory that the program uses while running, which results in a considerably larger dump file (potentially in the gigabyte range) than a stack dump. Note that a heap dump frequently contains case specific data, including data from the evidence.

> **Note:** For the quickest debugging of the crash, Guidance Software recommends selecting the Heap option.

Configuring Time Zone Settings

To configure time zone settings:

1. In a case, click the **Evidence** tab to view a list of your devices in the **Table** tab.
2. Click the name of the device you want to modify.
3. From the **Device** menu select **Modify time zone settings**. The Time Properties dialog displays.



4. Select the time zone that you want to use.
5. If the time zone supports Daylight Savings Time, and there are different rules for different years, EnCase automatically applies the proper rules for the particular year. To override this behavior, select **Use single DST offset**. This causes a single offset and enables you to choose the year for the correct bias.
6. Click **OK**. The time zone is listed in the **Report** tab for that device.

EnCase Folder Locations

The current path used to store user data, user application data, and global application data can be seen under **Paths** on the EnCase home page. All path locations are configurable.

Application Folder

The application folder contains files used by EnCase. User data and user configuration settings are not saved in this location. The default path for Windows 7, Windows 8, and Windows Vista is `\Program Files\EnCase8`.

Folder Name	Description
Certs	License certificates
Condition	Default conditions
Config	Application configuration options
Drivers	Application drivers
EnScript	Default EnScripts and EnPacks
Filter	Default filters
Help	Help files
Installers	EnCase installation executables
Lib	Application library files
License	EnLicense files
Mobile	Mobile phone drivers
Template	Default case templates

User Data

User-created files and backup user data are stored by Windows 7, Windows 8, and Windows Vista in the following default folder: `\Users\<Username>\Documents\EnCase`. The current path used to store user data displays under **Paths** on the EnCase home page.

Folder Name	Description
Cases	Individual case folders (described below)
Condition	User-defined conditions
EnScript	User-defined EnScripts
Evidence Cache	(see below)
Filter	User-defined filters
Keys	Encryption keys
Keyword	User-defined keyword searches
Logs	Console logs
Search	User-defined searches
Template	User-defined case templates

Case Backup

Backup case data are saved in the following location for Windows 7, Windows 8, and Windows Vista operating systems: `\Users\<Username>\Documents\EnCase\Cases\Backup`.

Case Folder

Case files are stored in the following default location for Windows 7, Windows 8, and Windows Vista operating systems: `\Users\<Username>\Documents\EnCase\Cases\<Case Name>`.

Folder Name	Description
Corrupt Pictures	Corrupt pictures

Folder Name	Description
Email	Email thread database
Export	Default case export folder
Results	Results of search queries (stored in the `..<Case Name>\Results` folder)
Searches	Keyword search results (non-Evidence Processor)
Tags	Tag database
Temp	Default case temporary folder
<Case Name>.Case	EnCase case file

Evidence Cache

The evidence cache folder contains the cache, index, and Evidence Processor results for a device. The default location for Windows 7, Windows 8, and Windows Vista operating systems is: `\Users\<Username>\Documents\EnCase\Evidence Cache\<Hash>`.

User Application Data

Configuration files and temporary user files associated with a specific user and EnCase installation folder are stored in the following location for Windows 7, Windows 8, and Windows Vista operating systems: `\Users\<Username>\App Data\Roaming\EnCase\EnCase8-<#>\Config`.

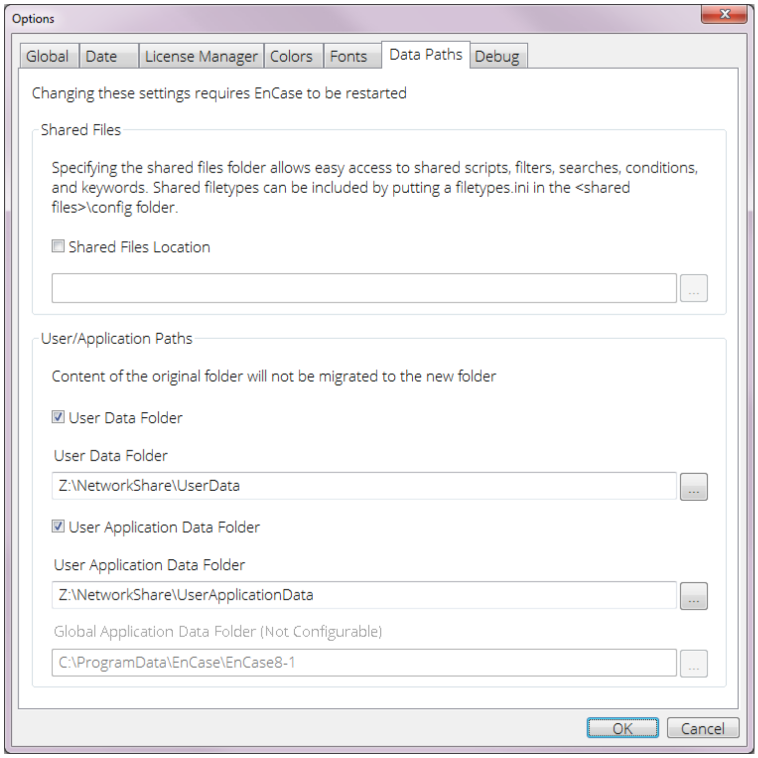
The current path used to store user application data displays under **Paths** on the EnCase home page.

Configuring a Windows Override Path

In normal operation, Microsoft Windows stores <User Application> and <User> data in specific locations on the boot (OS) hard drive. You can change these locations to any location on the boot hard drive, on a separate hard drive, or on a network share.

EnCase requires that these data locations have both read and write access. If Windows is set up so that either of these locations is on a read-only network share, or on a hard drive which is read-only and at a separate location, EnCase cannot store its settings correctly and cannot function properly.

To accommodate situations where you cannot change these locations, and the Windows store locations are read-only, EnCase allows you to change these locations for the EnCase application. You can change these locations by selecting **Tools** > **Options** > **Data Paths** tab. The Options dialog displays as shown here:



The User Data Folder is the default location for data such as cases, conditions, filters, logs and templates. The User Application Data Folder stores program settings and other configuration files.

Global Application Data

Global EnCase files are stored in the following location for Windows 7, Windows 8, and Windows Vista operating systems:

- `\Users\All Users\AppData\Roaming\EnCase`
- `\Users\All Users\AppData\Roaming\EnCase\EnCase8-<#>`

Note: `\Users\All Users\AppData` = `\ProgramData`

The current path used to store global application data displays under **Paths** on the EnCase home page.

Item	Description
Logos	Default report logo
Config	License Manager and other global configuration files
ParseCache	Parse cache files
Storage	EnScript configuration files

Install and Configure Evidence Processor Nodes

You can use the optional processor manager module in EnCase Examiner to distribute evidence processing jobs to other machines, or nodes, on your network. Each evidence processor node requires a software license or security key from Guidance Software. Evidence processor node licenses cost much less than a full EnCase Examiner license and can be a cost-effective way to increase the speed and efficiency of evidence processing. This section describes how to install the EnCase Processor Node executable on a machine for use as a processor node.

The processor manager module in EnCase Examiner enables you to manage, distribute, and monitor evidence processing jobs across your network. For information on using the processor manager, see Processor Manager on page 166. The processor manager and each processor node must have access to the shared drive where the evidence file and the cache are stored.

You can process evidence on any machine on your network, including other examiner machines. To enable a machine as an evidence processor, open the EnCase Processor Node executable file. This file installs the following two components:

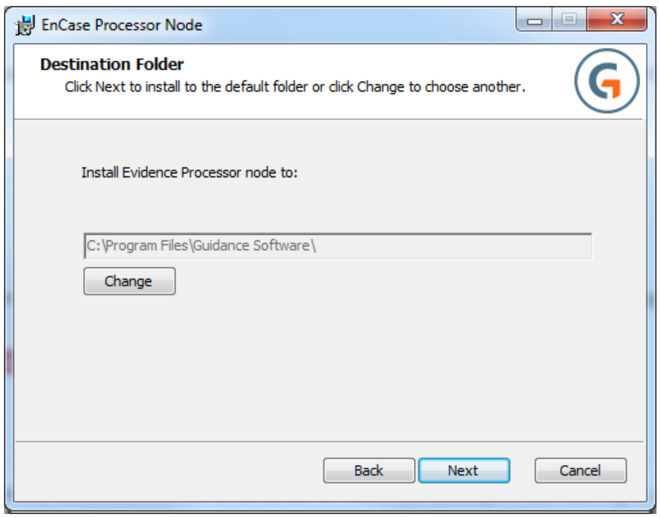
- **EnCase Processor Node** - Enables a machine to act as an evidence processor and accept work sent from the machine you use for processor management and examining evidence.
- **EnCase Processor Server (EnServer)** - A service that runs on a machine that enables communication between the node and the Processor Manager.

Once installed and configured, the machine will appear as an available node in your EnCase Examiner processor manager.

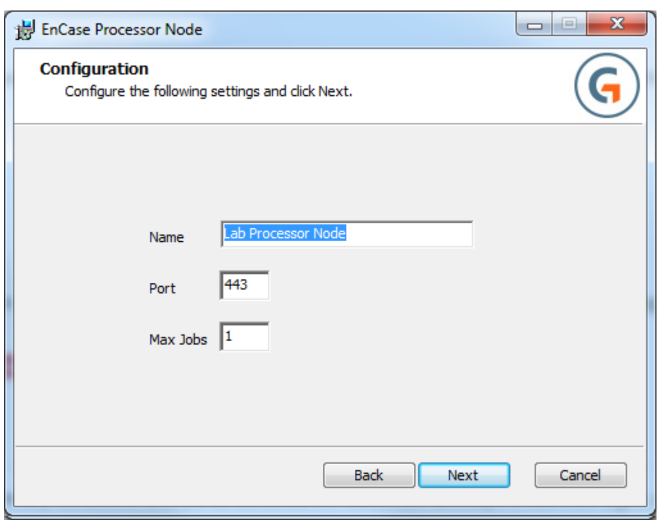
Note: Installing the evidence processor node on your local machine enables it to be used as a node by another examiner machine on your network.

To install the Evidence Processor Node:

1. Open the Evidence Processor Node executable file. The self-extractor dialog displays.
2. Click **Setup**. The Setup dialog displays.
3. Click **Next**. The Destination Folder dialog displays.

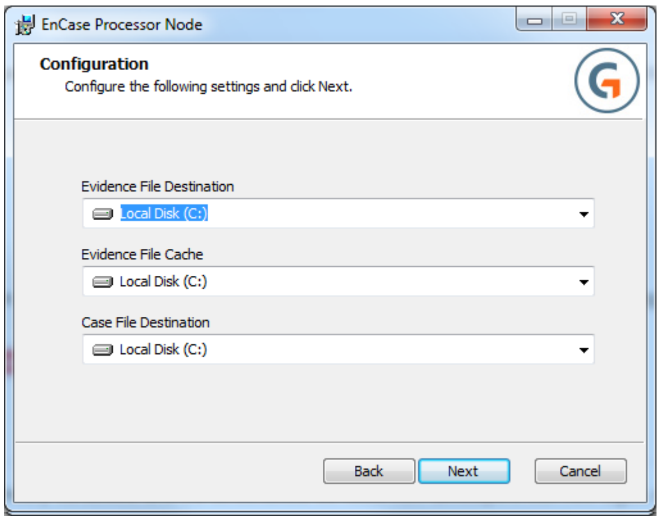


4. Accept the default path or click **Change** to enter another path, then click **Next**. The Configuration dialog displays.



- Give the node a meaningful name. This name displays in the Processor Node column of the Processor Manager tab.
- Enter the number of the port you want to use. The default is 443.
- You can execute multiple processing jobs simultaneously on a single processor node. Guidance Software recommends you leave the **Max Jobs** number set at 1.

5. Click **Next**. A second Configuration dialog displays.



- Specify the drives for the Evidence File Destination, the Evidence File Cache, and the Case File Destination.
- All paths must be specified in UNC format.
- For the Evidence File Cache, use the fastest I/O available.
- For detailed information about system requirements, see System Requirements on page 27.

Note: You can change these configuration settings after installation using the processor node Edit dialog. See Configuring Processor Nodes on page 168.

6. Click **Next**. A confirmation dialog displays.
7. Click **Install**. A dialog displays showing the progress of the installation.

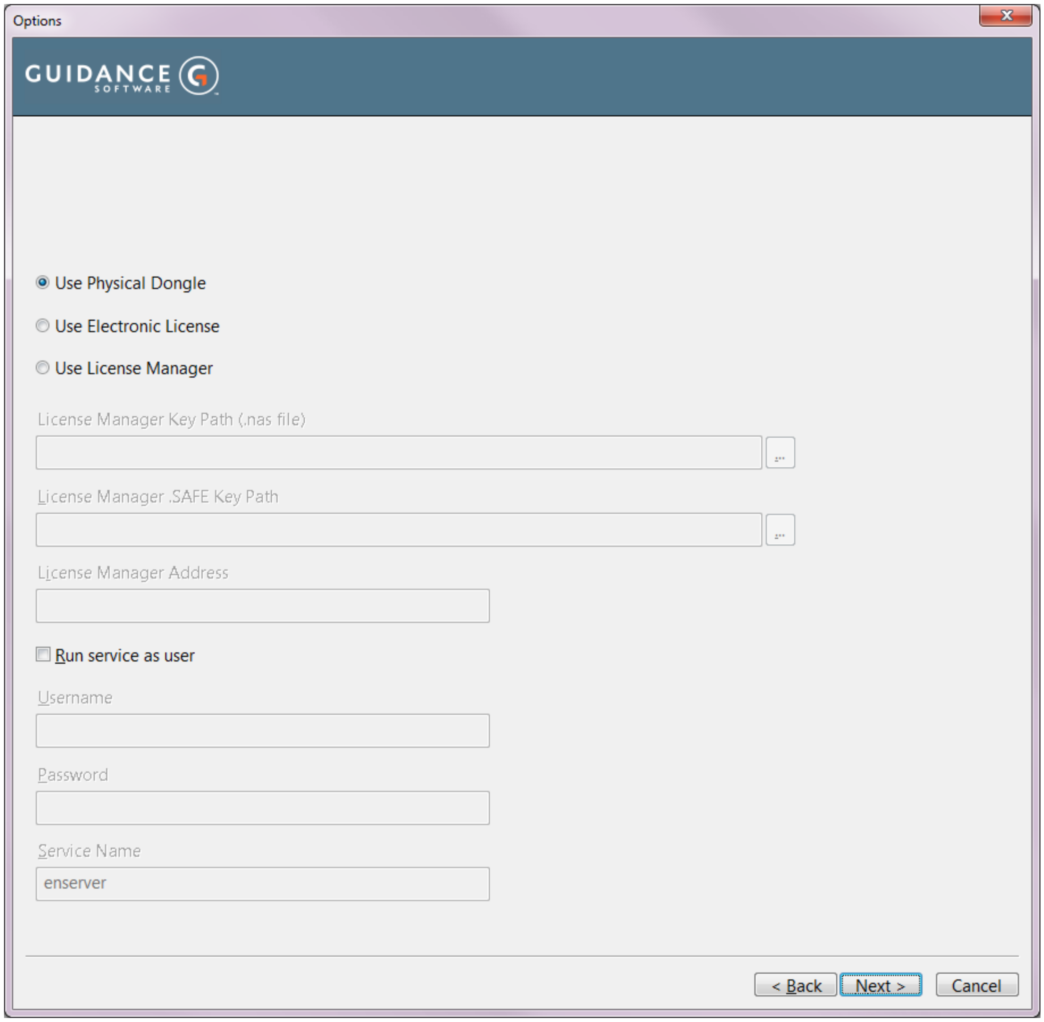
ENCASE SERVER INSTALLATION

After installing the EnCase processor node, the wizard begins the EnCase Processor Server (EnServer) installation process.

1. The EnCase Server Edition dialog displays after the processor node is installed.

Note: The EnCase Server Edition dialog may display behind another open dialog. If the process seems to be stuck after installing the processor node, look for the EnCase Server Edition dialog.

2. Accept the default install path or browse to another path, then click **Next**. The End User License dialog displays.
3. Select **I agree and accept**, then click **Next**. The Options dialog displays.



- Select the type of authentication you want to use.
  - If you are using License Manager, click **Use License Manager** and enter a License Manager Key Path, License Manager .SAFE Key Path, and License Manager Address.
- Select **Run service as user** if you do not want to run the service as a local system account.

- Enter a username and password.
- The user specified should have read permission to evidence and read/write permission to evidence caches to be processed by this Evidence Processor Node.

4. When done, click **Next**. The Installation Folder dialog displays.
5. Click **Next**. A bar displays showing progress of the EnServer installation. The Setup Complete dialog displays.
6. Click **Finish**. A dialog displays showing License Manager files are being copied, then the Evidence Processor Node Setup dialog displays, indicating the setup is complete.
7. Click **Finish**.

Checking the Windows Application Log

After installing the processor node and EnCase Processor Server (EnServer), open the Event Viewer in Windows by typing `eventvwr` in a Windows command line.

The Windows Application log should display:

- A log entry for EnServer starting.
- A log entry showing the dongle ID given to the EnCase Processor Server (EnServer).
- If installed, a log entry for License Manager.
- A log entry showing your security key (dongle) type (for example, Forensic).
- A log entry showing "EnServer running."

You may also see an error stating "...restarting script...EnServer." This displays when you manually start the EnCase Processor Server service.

All of the logs listed above should be present; if not, EnCase Processor Server started, then stopped, and is offline.

CHAPTER 2

USING PATHWAYS TO STREAMLINE WORKFLOWS

Pathways Overview 59

Using a Pathway to Create a Full Investigation 59

Using a Pathway to Preview and Triage your Evidence 63

Custom Pathways 66

Pathways Overview

Pathways provide step by step guidelines to walk you through specific workflow scenarios. Each Pathway contains links that take you to individual steps in the workflow process.

Pathways are based on the curriculum taught by the award-winning Guidance training department, and are designed to help examiners of any level efficiently navigate an investigation. Pathways are not mandatory. You can exit a Pathway at any stage of your investigation.

You can access Pathways from two locations in the interface:

- Home page
- Toolbar menu

If you exit the Pathway, or your workflow navigates you away from the Pathway, you can always return to the Pathway from one of these two access points.

Using Pathways you can:

- Create a full investigation
- Preview and triage your evidence

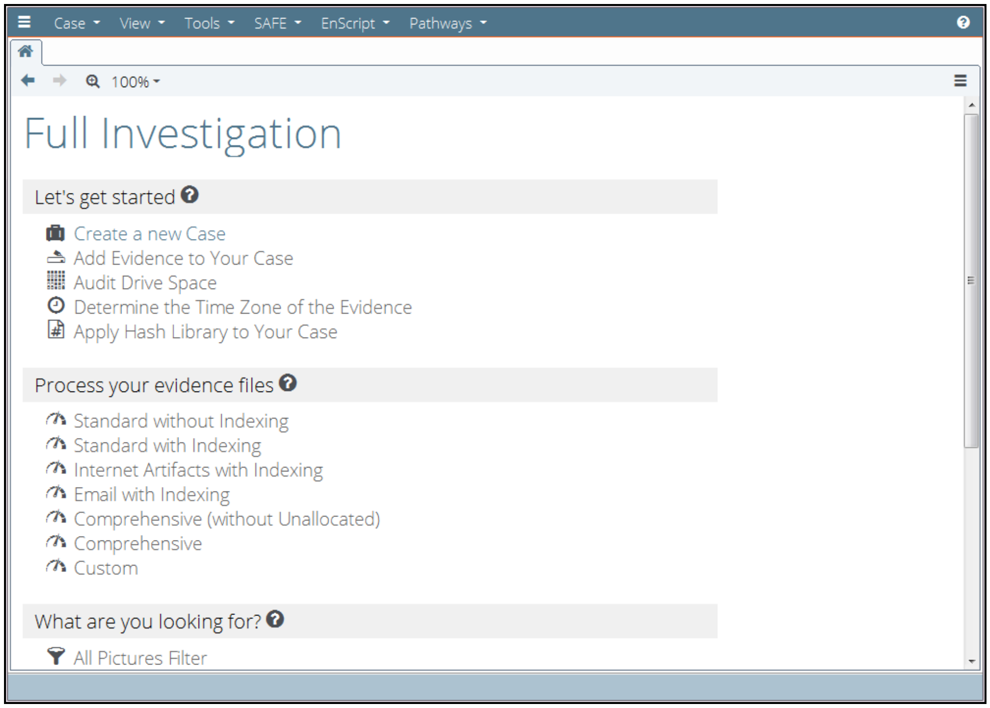
Using a Pathway to Create a Full Investigation

GETTING STARTED

To get started with a full investigation, the Pathway suggests five steps:

- Create a case
- Add evidence
- Audit your drive space
- Determine the time zone of your evidence
- Apply a hash library to your case

1. On the home page in the Pathways group, click **Full Investigation**.
2. The Full Investigation page displays.



3. You can follow the steps for the case you have open, or you can start a new case by clicking **Create a New Case**. See Using a Case Template to Create a Case on page 79.
4. Once you create a case, the next step is to add evidence to it. Back on the Full Investigation page, click **Add Evidence to Your Case**. The Add Evidence dialog displays.
5. Click the appropriate link and follow the instructions to perform any of the available add evidence actions. This must be done before any processing is done on the evidence. See Adding Evidence to a Case on page 82.
6. After evidence is added, the next step is to audit the space of all devices in the case. This must be done before any processing is performed on the evidence. This process builds a summary table in the bookmarks tab showing the usage of all devices in the case. Additional tables are built in the bookmarks tab for each device to account for all space on each drive. See Audit Drive Space on page 107.
7. Now that your drive space is audited, the Pathway leads you towards setting a time zone for your evidence. This step parses the System Registry Hive to determine the current control set and then parses the current control set to retrieve the time zone information for each of the selected evidence files. To preserve the forensic accuracy of the data, this must be done before any processing is done on the evidence. In the Full Investigation dialog, click **Determine the Time Zone of the Evidence**. See Determining the Time Zone of Your Evidence on page 224.

8. On the Full Investigation page, click **Apply Hash Library to Your Case**. See Adding Hash Libraries to a Case on page 288.

PROCESSING EVIDENCE

Once you have set up your case and added evidence, you can process it in a variety of ways. Once you have processed your evidence with one of the processing profiles listed below, you will be unable to reprocess it with another Pathway Profile. Any further processing should be done using the Custom profile option.

Once a processing profile is selected, you can view its progress by double clicking the progress bar on the bottom right of the screen.

- Process evidence without indexing (fastest)
  - File signature analysis
  - Hash analysis (MD5 and SHA-1)
  - Expand compound files
  - Find email (except lost or deleted items)
  - Find allocated Internet artifacts
  - System Information Parser without live registry
  - Allocated Windows artifacts
- Process evidence with indexing
  - File signature analysis
  - Hash analysis (MD5 and SHA-1)
  - Expand compound files
  - Find email (except lost or deleted items)
  - Find allocated Internet artifacts
  - Index allocated text and metadata (with East Asian script support)
  - Skipping files in hash library and skipping slack
  - System Information Parser without live registry
  - Allocated Windows artifacts
- Process Internet artifacts
  - File signature analysis
  - Hash analysis (MD5 and SHA-1)
  - Find allocated Internet artifacts
  - System Information Parser without live registry
- Process email
  - File signature analysis
  - Hash analysis (MD5 and SHA-1)
  - Expand compound files
  - Find email (except lost or deleted items)
  - Index allocated text and metadata (with East Asian script support)
  - Skipping files in hash library and skipping slack
  - System Information Parser without live registry

- Comprehensive processing without unallocated (for deep investigation of allocated files)
  - Recover folders and NTFS 3.0 reconstruction
  - File signature analysis
  - Protected file analysis
  - Expand compound files
  - Find email (except lost or deleted items)
  - Find allocated Internet artifacts
  - Index allocated text and metadata (with East Asian script support)
  - Skipping files in hash library and skipping slack
  - System Information Parser without live registry, all advanced folders
  - Allocated Windows artifacts
  - Protected file analysis
  - Thumbnail creation
- Comprehensive processing (for deep investigation of an entire drive)
  - Recover folders and NTFS 3.0 reconstruction
  - File signature analysis
  - Hash analysis (MD5, SHA-1 and entropy)
  - Expand compound files
  - Find email (except lost or deleted items)
  - Find all Internet artifacts, including unallocated
  - Index allocated text and metadata (with East Asian script support)
  - Skipping files in hash library and skipping slack
  - System Information Parser without live registry, all advanced folders
  - All Windows artifacts, including unallocated
- Custom: Use this to build your own processing routine

WHAT ARE YOU LOOKING FOR?

Once you process your evidence files, you can now find information in a variety of ways.

- Select the filter options to find information by type or specific attributes:
  - All pictures finds all files with image extensions
  - All documents finds all files with document extensions
  - All files over specified size enables you to specify a logical size value and find all files exceeding that value
  - All files by extension enables you to define specific extensions to search for
- Select the view options to see different aspects of your evidence. These options only work if email messages and/or internet artifacts were selected during processing. Selecting either one of these options takes you to the **Artifacts** tab.
  - View email messages
  - View Internet artifacts

- Select the search options to perform:
    - Index searches (Indexing must have been included in the selected processing option.)
    - Keyword searches (Selecting this option opens the **Search** view; select the Keyword tab to view the live results.)

GENERATING REPORTS

After you have found the information you need, you can generate reports in a variety of ways.

- Generate a standard full examination report
- Report templates enable you to create a customized report. See Using Report Templates on page 397.
- Generate a Triage report to easily share your findings in HTML format. See Triage Report on page 390.

Using a Pathway to Preview and Triage your Evidence

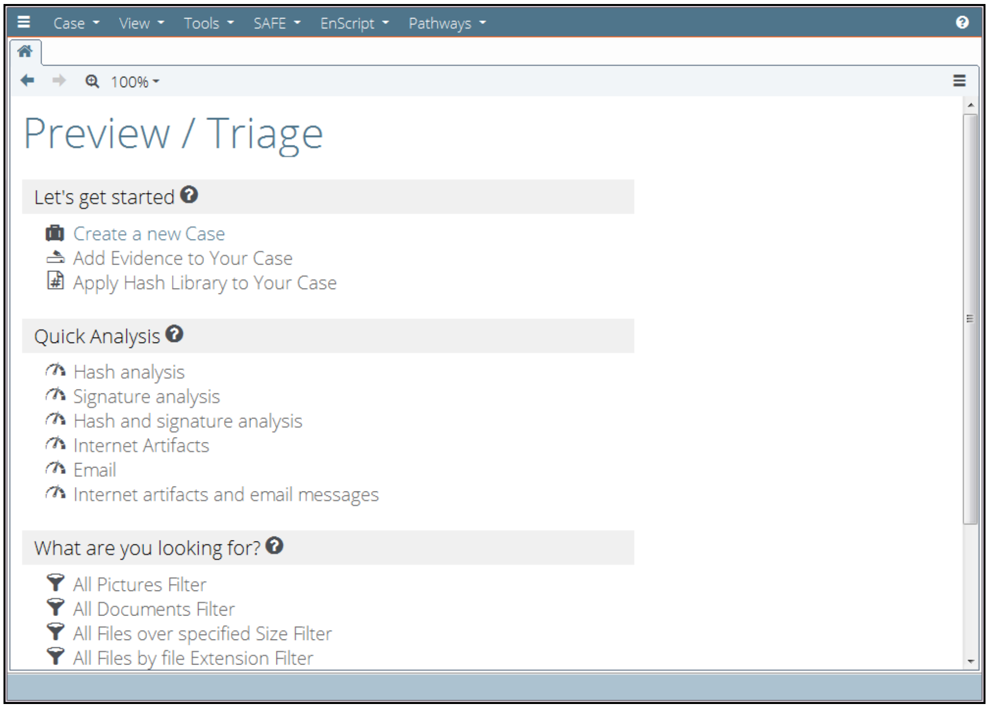
The Preview/Triage pathway helps you to easily preview and triage your evidence.

GETTING STARTED

To get started with a triage case, the pathway suggests three steps:

- Create a case
- Add evidence
- Apply a hash library to your case

1. On the home page in the Pathways group, click **Preview/Triage**.
2. The Preview / Triage page displays.



3. You can follow the steps for the case you have open, or you can start a new case by clicking **Create a New Case**. See Using a Case Template to Create a Case on page 79.
4. Once you create a case, the next step is to add evidence to it. Back on the Preview/Triage page, click **Add Evidence to Your Case**. The Add Evidence dialog displays.
5. Click the appropriate link and follow the instructions to perform any of the available add evidence actions. See Adding Evidence to a Case on page 82.
6. On the Preview/Triage page, click **Apply Hash Library to Your Case**. See Adding Hash Libraries to a Case on page 288.
7. The Apply Hash Library to Case dialog displays.

QUICK ANALYSIS

Once you have set up your case and added evidence, you can process it in a variety of ways:

- Perform hash analysis
  - Hash analysis (MD5 and SHA-1)
- Perform signature analysis
  - File signature analysis

- Perform hash and signature analysis
  - File signature analysis
  - Hash analysis (MD5 and SHA-1)
- Locate Internet artifacts
  - Find allocated Internet artifacts
- Locate email messages
  - Find email (except lost or deleted items)
- Locate Internet artifacts and email messages
  - Find email (except lost or deleted items)
  - Find allocated Internet artifacts

WHAT ARE YOU LOOKING FOR?

Once you process your evidence files, you can now find information in a variety of ways.

- Select the filter options to find information by type or specific attributes:
  - All pictures finds all files with image extensions
  - All documents finds all files with document extensions
  - All files over specified size enables you to specify a logical size value and find all files exceeding that value
  - All files by extension enables you to define specific extensions to search for
- Select the view options to see different aspects of your evidence:
  - View email messages
  - View Internet artifacts

GENERATING REPORTS

After you have found the information you need, you can:

- Generate a Triage report to easily share your findings in HTML format. See Triage Report on page 390.

Custom Pathways

Custom pathways are sequences of options that can be configured to match your specific workflow. Options in a pathway can consist of EnScript instructions, filters, and conditions. Headers can be added to provide help information.

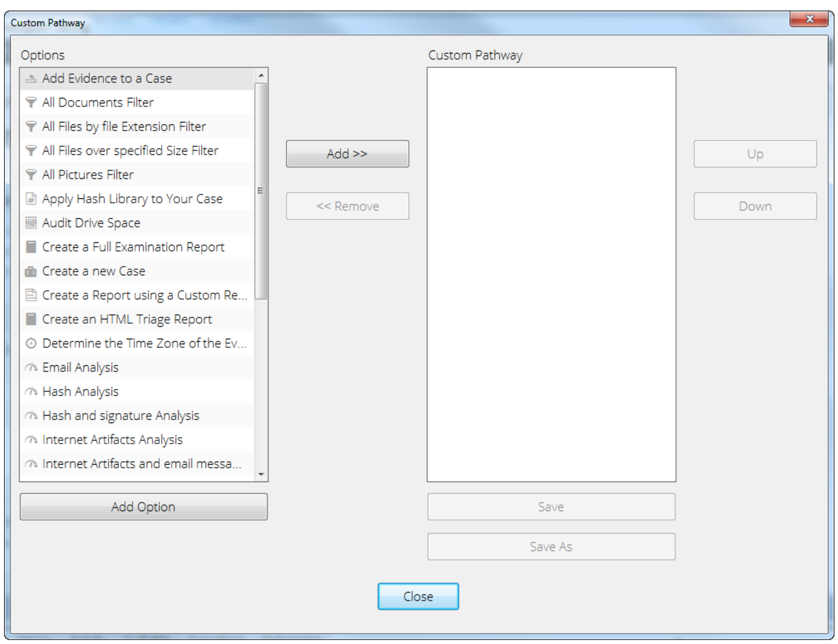
The topics below detail how to:

- Create a custom pathway
  - Add options to the custom pathway
  - Add EnScript files, filters, conditions, and help information to your current list of options
  - Save your pathway
- Edit and delete a custom pathway
- Create and edit a custom pathway header

Creating a Custom Pathway

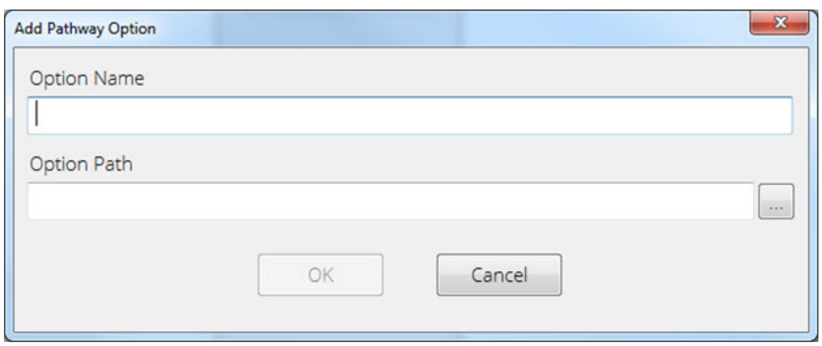
To create a custom pathway:

1. In EnCase Forensic, navigate to the **Pathways** dropdown menu and select **Create New**. The Custom Pathway dialog displays.



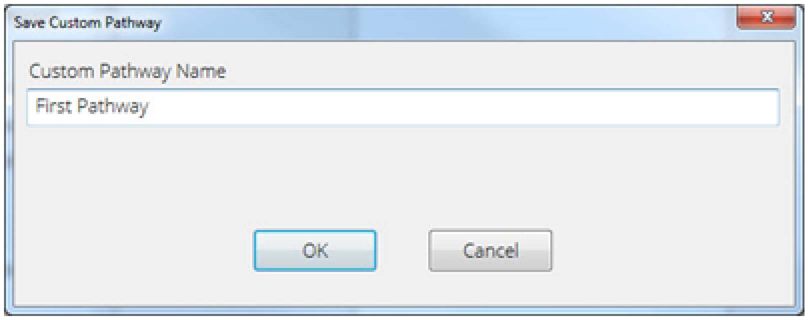
- The left pane displays all available options (alphabetically) that can be added to a custom pathway.
    - By default, this list is populated with the options found in the standard Full Investigation and Preview/Triage pathways.
    - Options can be created by calling EnScript files, pre-configured filters, EnPacks, conditions, and header help files.
- The right pane displays the options currently included in your new custom pathway.
- To add options to your custom pathway, select an item from the left pane and click **Add**.
- To remove options from your custom pathway, select an item from the right pane and click **Remove**.
- Use the **Up** and **Down** buttons to rearrange options in the custom pathway you are building. You can arrange options in a pathway in any order.

2. To add a new option to the Options list, click **Add Option**. The Add Pathway Option displays.



- Enter a descriptive name in the Option Name field.
- Click the **Browse** ellipses button in the Option Path field to open a file browser, then navigate to the existing EnScript, EnPack, condition, filter, or help file that you want to use for this option.
- When done, click **OK**.
    - The new option displays in the left pane of the Custom Pathways dialog.
    - To delete a custom option, right click on the option and select **Delete**.

3. When you finish building your custom pathway, click **Save As**. The Save Custom Pathway dialog displays.



4. Give the pathway a title and click **OK** to save it.

Once saved, the pathway displays in both the Pathways dropdown menu and on the home page.

To access a custom pathway:

1. Click **Pathways**, then click the name of the custom pathway you created.
2. The pathways you created display as links. Action links require a case to be open for them to be active; if no case is open, the links are not clickable. Action link types are:
    - EnScripts (*.EnScript)
    - EnPacks (*.EnScript)
    - Conditions (*.EnCondition)
    - Filters (*.EnFilter)

    Note that:

- Pathway Help Files (*.txt) are not action links.
- **Create a New Case** is always available.
- **Determine the Time Zone of the Evidence** is only available if a case is open and there is evidence in the case that has not been processed.
- **Search Index** is only available if the evidence has been processed with indexing turned on.

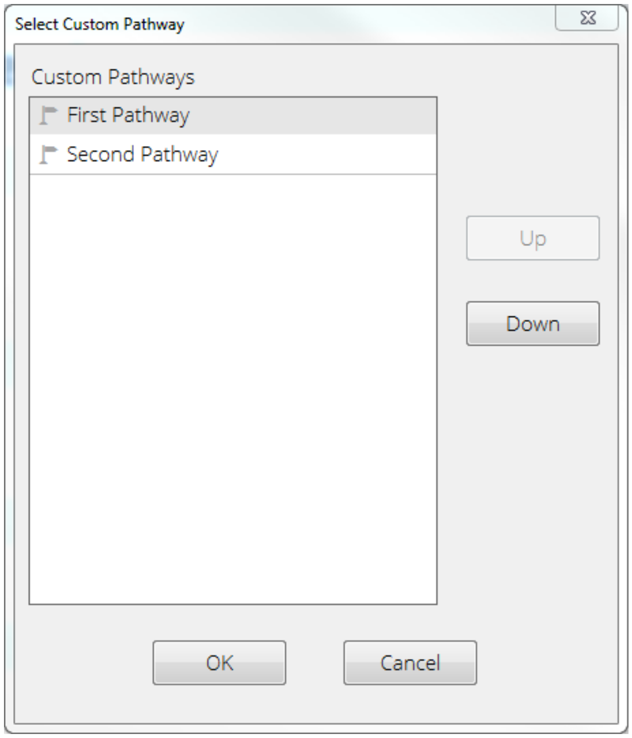
Modifying a Custom Pathway

You can edit and delete custom pathways.

To edit a custom pathway:

1. In EnCase Forensic, navigate to the **Pathways** drop down menu and select **Edit**/**Delete Pathway** > **Edit Pathway**.

- If only one pathway exists, the pathway displays in the edit dialog.
- If multiple pathways exist, the Select Custom Pathway dialog displays.



- Select the pathway you want to edit.
- The **Up** and **Down** buttons change the order in which the pathways are displayed.

2. When done, click **OK**. The Custom Pathway dialog displays the custom pathway you have selected.
3. Modify your custom pathway as desired.
4. When done, click **Save As** to create a new pathway with your updated changes, or click **Save** to save the changes to your original pathway.

Your new custom pathway now displays in the Pathways dropdown menu and in the Pathways area of the home page.

To delete a custom pathway:

1. In EnCase Forensic, navigate to the **Pathways** drop down menu and select **Edit**/**Delete Pathway** > **Delete Pathway**. The Select Custom Pathway dialog displays.
2. Select the pathway you want to delete and click **Delete**.

    - A dialog displays confirming you want to delete this pathway. Click **Yes**.

- After you confirm, the Delete Pathway dialog remains open so you can delete additional pathways if desired. When you finish deleting pathways, click **Close**.

Deleted pathways no longer display on the home page or the Pathways menu.

Using Custom Pathway Headers

Custom pathway headers enable you to embed helpful information within the workflow of your pathway. This provides structure as well as helpful text.

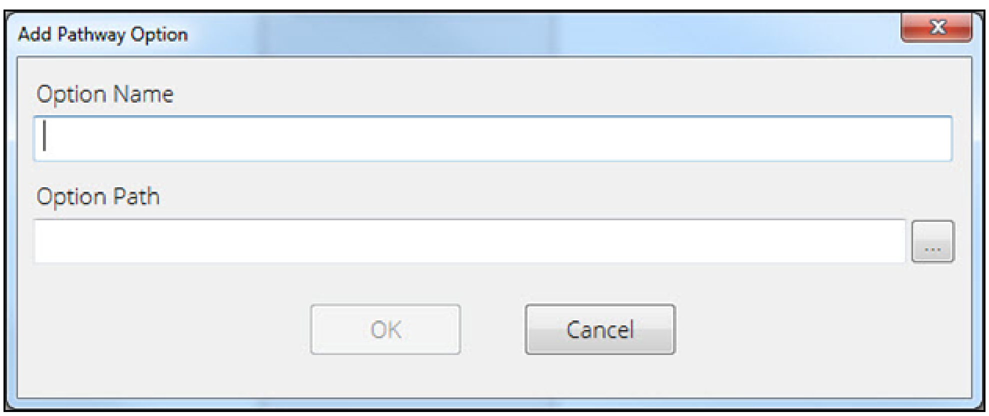


The header name is displayed in the workflow. When you click the **?** icon next to the name, the associated help file displays in a popup dialog.

Pathway headers are .txt files which can be added in the same way as other options.

To create a custom pathway header:

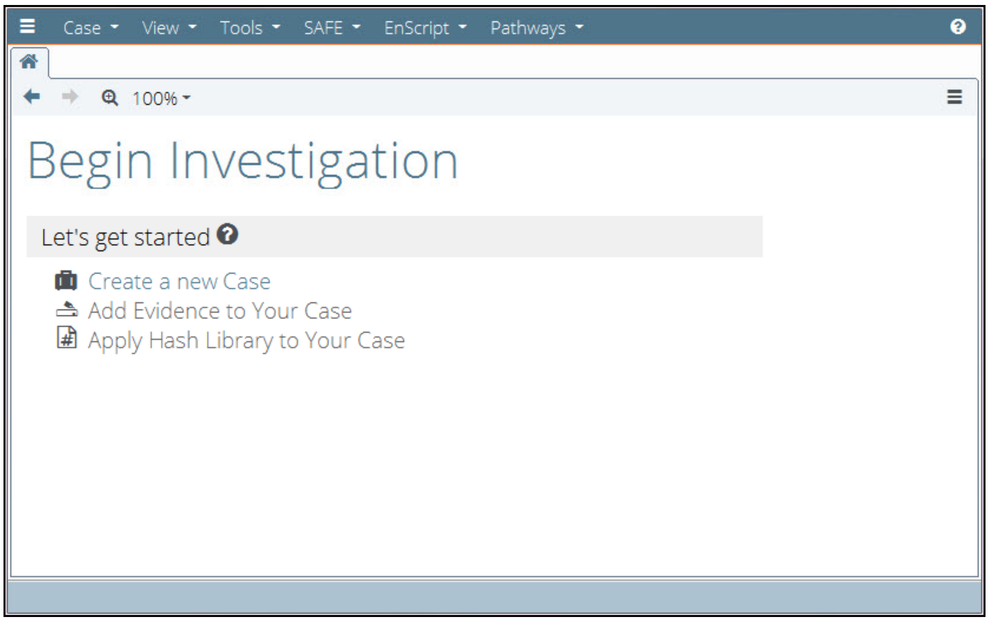
1. From the Pathway Options list, click **Add Option**. The Add Pathway Option displays.



- Enter a descriptive name in the Option Name field.
- Click the **Browse** ellipses button in the Option Path field to open a file browser, then navigate to the existing help .txt file that you want to use.

- When done, click **OK**.
  - The new option displays in the left pane of the Custom Pathways dialog.
  - To delete a custom option, right click on the option and select **Delete**.

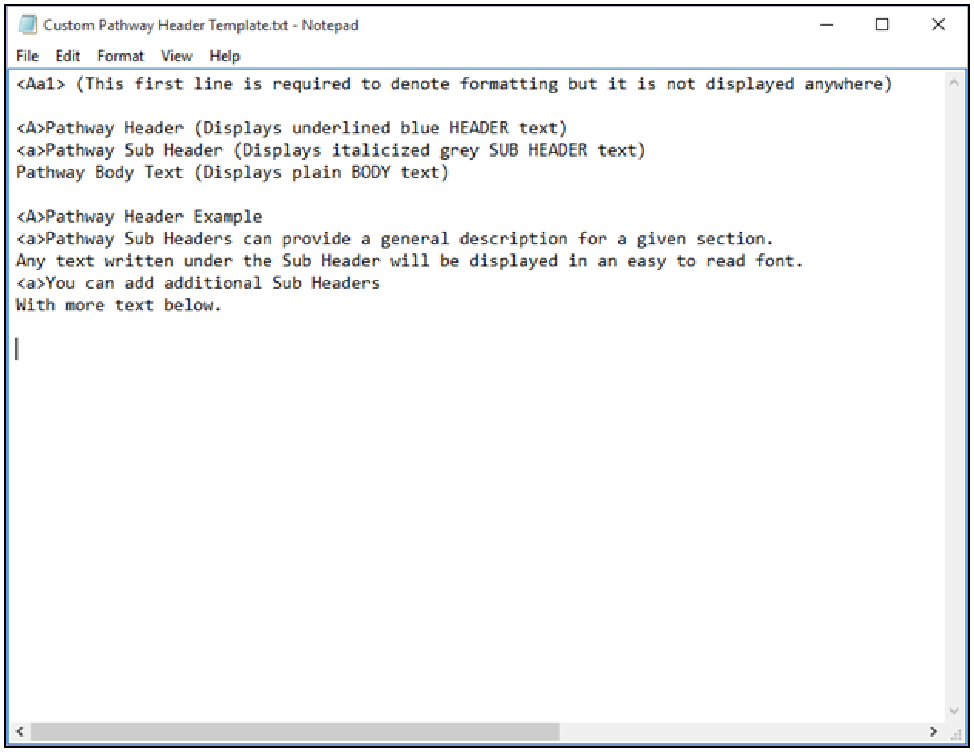
The header name displays within the structure of the pathway. When you click the **?** icon next to the name, the associated help file displays in a popup dialog.



To create a header file:

Header files are .txt files that can contain some basic formatting.

A sample template is installed at `<EnCase Install Path>\Template\Pathway\Custom Pathway Header Template.txt.`

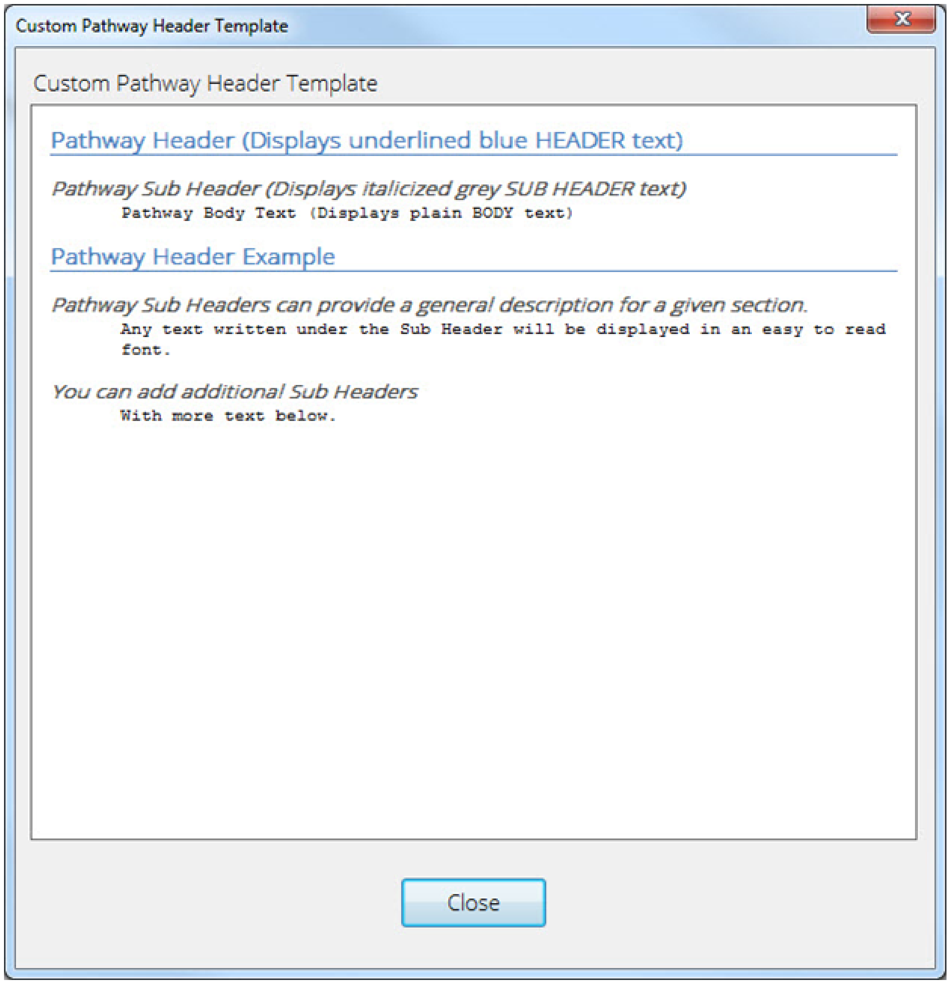



```
<Aa1> (This first line is required to denote formatting but it is not displayed anywhere)

<A>Pathway Header (Displays underlined blue HEADER text)
<a>Pathway Sub Header (Displays italicized grey SUB HEADER text)
Pathway Body Text (Displays plain BODY text)

<A>Pathway Header Example
<a>Pathway Sub Headers can provide a general description for a given section.
Any text written under the Sub Header will be displayed in an easy to read font.
<a>You can add additional Sub Headers
With more text below.
```

The formatting of this template creates a help dialog that looks like this:


Custom Pathway Header Template
Custom Pathway Header Template
Pathway Header (Displays underlined blue HEADER text)
Pathway Sub Header (Displays italicized grey SUB HEADER text)
Pathway Body Text (Displays plain BODY text)
Pathway Header Example
Pathway Sub Headers can provide a general description for a given section.
Any text written under the Sub Header will be displayed in an easy to read font.
You can add additional Sub Headers
With more text below.
Close

CHAPTER 3

WORKING WITH CASES

Overview	77
Launching EnCase	77
Using a Case Template to Create a Case	79
Adding Evidence to a Case	82
Case Operations	85
Case Portability	87
Case Page Logo	88

Overview

This chapter describes how to use EnCase to create and start work on a case. It explains the major components of the user interface, and how to use them to take full advantage of EnCase features.

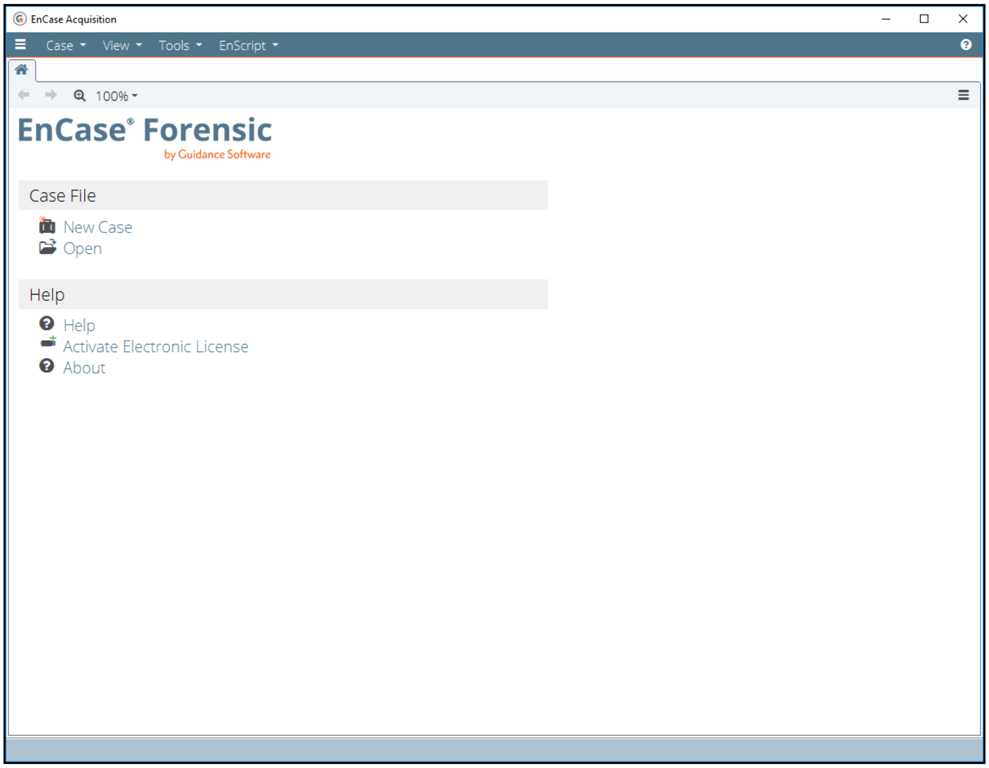
The chapter's purpose is to get you started with EnCase case creation. This chapter:

- Explains how to use the main features of this digital forensic tool.
- Describes the structure used to gather and process case evidence.
- Guides you through the initial stages of case creation.
- Introduces you to the basics of using case templates.
- Describes the process of adding evidence to a case and setting case options.
- Shows how to work with cases.
- Describes the case portability feature.

In EnCase, a case is stored in a folder, with subfolders for case-specific information such as tags and search results. The case folder and the components contained within that folder directly associate the investigative work you perform with the evidence. As a result, the case folder should not be directly opened or modified.

Launching EnCase

When you launch EnCase, the Home page displays.



The Home page, like all EnCase pages, consists of several sections, each with a specific set of functions. In descending order, they are:

Application Toolbar	Displays below the title bar and provides dropdown menus to major areas of functionality. The menus and their selections remain static throughout your investigation. Later sections in this chapter describe them in more detail.
Tabs	Displays a page that groups a portion of EnCase functions, similar to tabs in Internet browsers. When you open EnCase for the first time, only the **Home** tab displays.

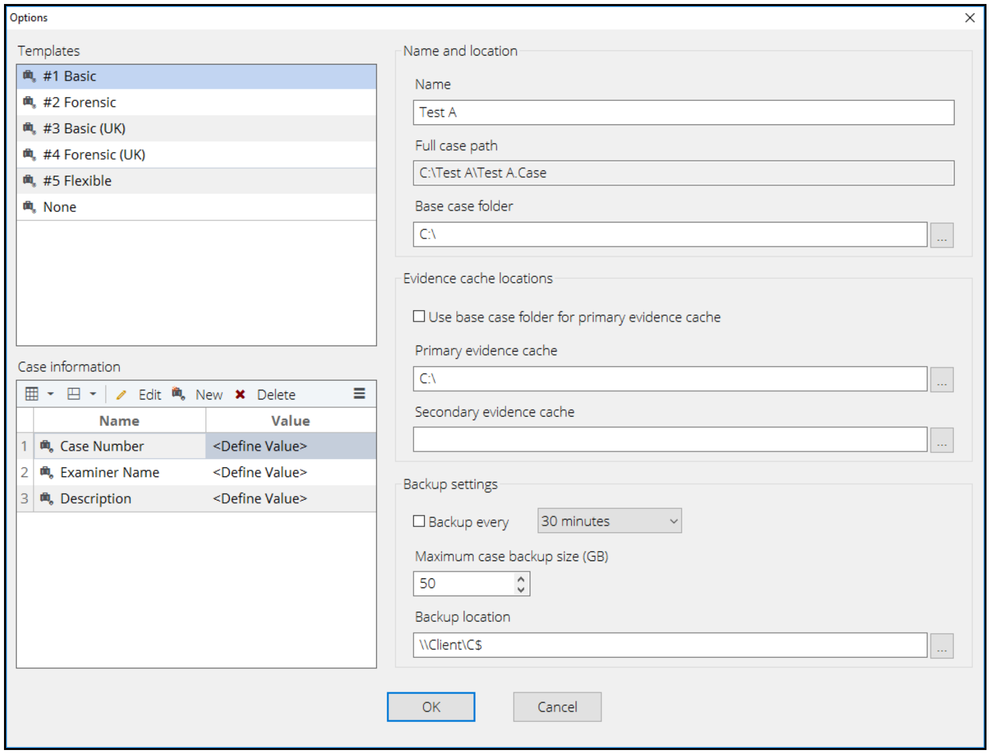
Tab Toolbar	Contains menus and buttons specific to the selected tab. Includes back and forward arrows, which function the same as in browsers, and options that allow you to resize the panel.
Page Body	Displays content according to the tab you are viewing. On the Home page, the page body consists of a label that identifies the product, the case, and available functions. Sections identify categories of EnCase components with links to the features and actions available within each category.

Using a Case Template to Create a Case

After installing and configuring EnCase, you can create a new case with an EnCase supplied case template. Following are instructions for creating a new case with a case template. After you create a case, most of the EnCase features and their navigation paths become available. You begin creating a case under the FILE category of the **Home** tab.

To create a new case:

1. Click **New Case** beneath the CASE FILE category on the **Home** tab.
2. The Case Options dialog displays. Use this dialog to select a case template and name the case.
3. In the figure below, the **#1 Basic** template is selected.
4. Enter a case **Name**, then click **OK**.



Case Options Settings

- **Name**: A text string you enter to identify the case file. A case is a folder containing many components, such as folders for temporary directories, tags, and search results. The name specified in this field is used to name the case folder, as well as components contained in that folder.
- **Full case path**: The folder where the case file is stored. This path is determined by the **Base case folder**, followed by a subfolder with the case name.
- **Base case folder**: The location where the above case folder is created. By default, EnCase uses a folder beneath your My Documents folder.
- **Use base case folder for primary evidence cache**: Check this box if you want to use the base case folder specified above for the case's primary evidence cache. If you select this option, the **Primary evidence cache folder** field is disabled.
- **Primary evidence cache**: EnCase Version 8 uses cache files to speed up application responsiveness, enhance stability, and provide scalability across large data sets. The primary evidence cache folder is where EnCase saves and/or accesses these files. You can create cache files in advance through the Evidence Processor, and you can point to the folder that contains this cache data. Although there is an evidence cache for each device in a case, the evidence cache does not need to be stored with the evidence files. If cache

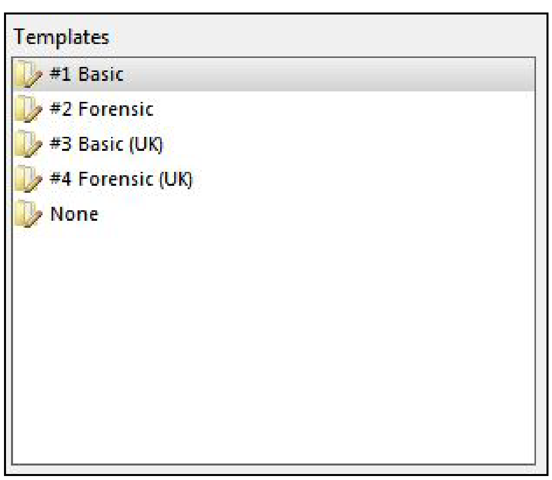
files were not created for a device, they are stored in this folder when the Evidence Processor is run.

- **Secondary evidence cache**: EnCase allows you to specify a secondary location for a previously created evidence cache. This allows you to specify a folder on a network share or other location to store cache files. Unlike the primary evidence cache folder, EnCase reads previously created files from this location only. Evidence caches which do not exist in the Secondary folder are stored in the Primary folder. Previously existing evidence caches in the Secondary folder continue to be stored in the Secondary folder.
- **Backup every 30 minutes**: Click the checkbox to set up backups at 30 minute intervals. Click the up/down arrows on the **Maximum case backup size (GB)** field to set the maximum case backup size.
- **Backup location**: The folder where case backup data is stored.
- **Case information**: Case information items are user configurable name-value pairs that document information about the current case. Primarily, you use this user definable information to insert into a Report. To create case information items, click the **New** button on the toolbar. To edit case information items, select an item and click the **Edit** button on the toolbar.

Click **OK** to apply the case options. The **Home** tab then displays a page for this particular case with the case name at the top. This case page lists hyperlinks to many common EnCase features and you can use it as the control center for this case. You are now ready to begin building your case.

Case Templates

When you create a new case, EnCase displays a list of available templates. These are `.CaseTemplate` files. EnCase supplies several predefined templates, using the pound sign (#) as a prefix. Their names display in this box along with any saved templates.



Click a name from the case **Templates** list to select it.

Although you can configure a new case using the blank template (**None**), Guidance Software recommends using a template, as it simplifies the case creation process. Each case template contains a uniquely configured set of the following elements:

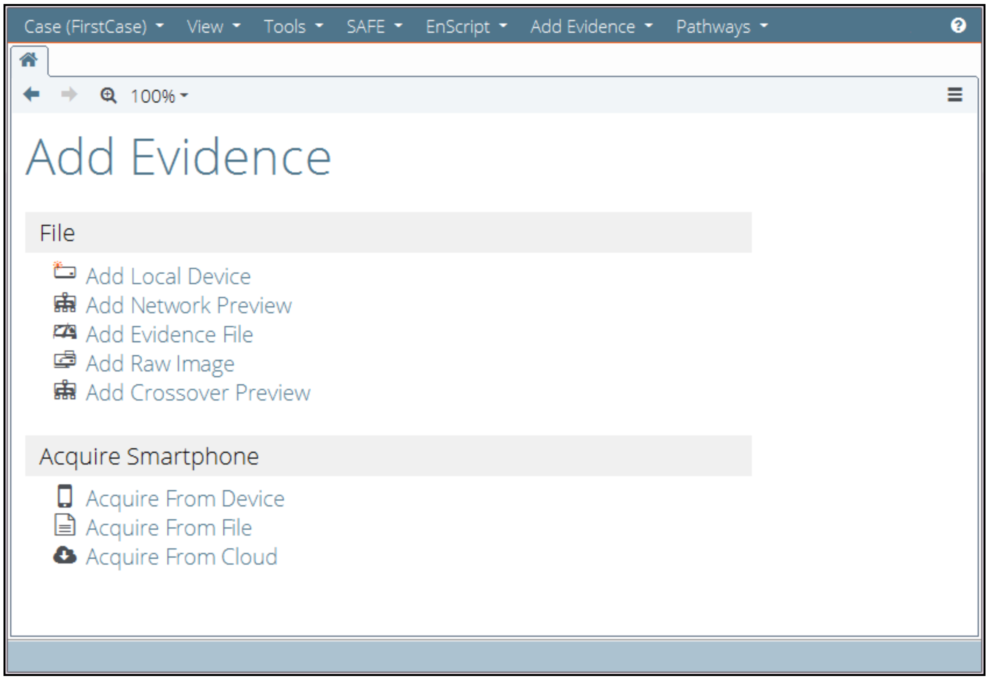
- Case Info items with default values
- Bookmark folders and notes
- Tags
- Report templates
- User-defined report styles

You can also create your own templates by saving any case as a template. Afterwards, the new template displays in the Templates list and is available for future use. If you intend to create a number of cases with a similar structure, save one of them as a template and use it to generate the other cases. You can share case templates with other users by sending them the case template file.

Adding Evidence to a Case

Once a case is created, you can add evidence to it by selecting the **Add Evidence** hyperlink on the case page, or by selecting the **Add Evidence** dropdown menu from the application toolbar.

If you click the **Add Evidence** link on the Case page, the page changes to one like that shown below. At any time, you can use the back or forward buttons to help navigate through the different **Home** tab pages.



The **Add Evidence** menu contains these selections and a selection to open the Evidence Processor. For more information, see the Evidence Processor Overview.

The following evidence selections are available:

- **Add Local Device**: Initiates the process of adding a local device attached directly to your local computer. This can be the main system drive, a device attached through a Tableau write blocker, any other device connected to an internal bus connection, floppy drives, optical media, card readers, or any device connected to a USB port.
- **Add Network Preview**: Select one of two acquisition options: **Add SAFE Network Preview** or **Add Direct Network Preview**.
- **Add Evidence File**: Specifies an evidence file to add to the active case. This can be an EnCase Evidence file (E01 or Ex01), Logical Evidence file (L01 or Lx01), VMWare (vmdk), Virtual PC file (vhd), or SafeBack (*.001) file.
- **Add Raw Image**: Adds a raw or dd image file of a physical device to the active case.
- **Add Crossover Preview**: Crossover cable acquisitions require both a subject and examiner machine. This type of acquisition also negates the need for a hardware write blocker. It may be desirable in situations where physical access to the subject machine's internal media is difficult or is not practical. This selection is the recommended method for acquiring laptops and exotic RAID arrays.
- **Process Evidence**: Allows automated processing of case evidence across a wide selection of parameters. This option is available only when one or more evidence items are added to the case.
  The Evidence Processor includes features such as:

- ◦ Analyzing file signatures. See Analyzing File Signatures on page 138.
- ◦ Creating an index of the case evidence data. See Creating an Index on page 148.
- ◦ Searching for email threads and conversations. See Finding Email on page 139.
- ◦ Searching Internet artifacts. See Finding Internet Artifacts on page 139.

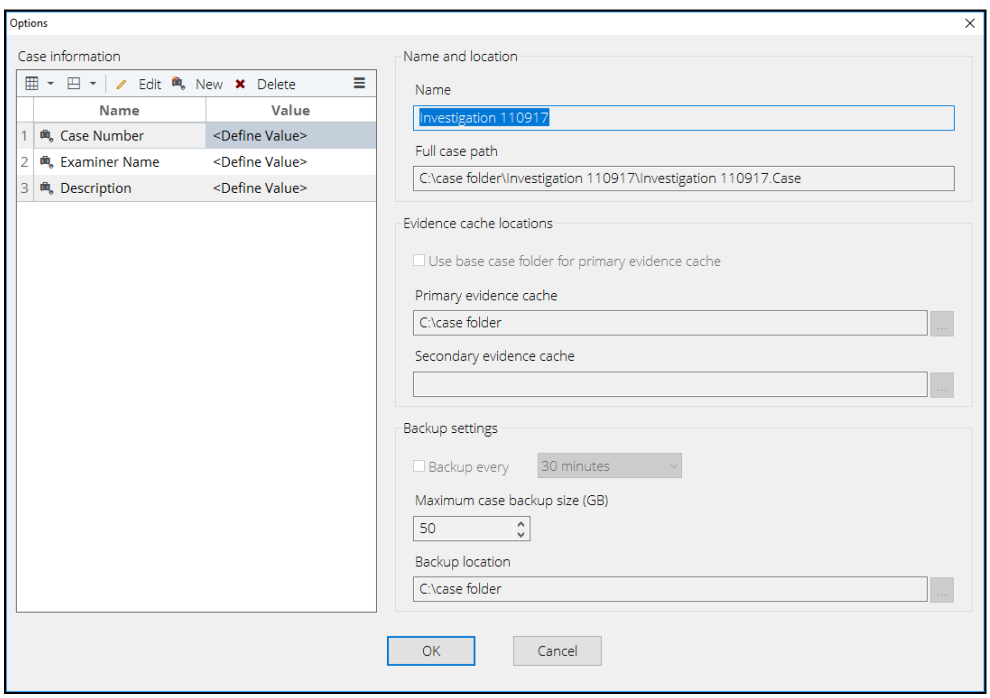
There are additional options for acquiring mobile devices under **Acquire Smartphone**:

- **Acquire from Device**: Opens the Acquisition Wizard, which detects the mobile device you have plugged in to your computer and walks you through the acquisition process.
- **Acquire from File**: Opens the Import Wizard, which allows you to import a backup file from a mobile device.
- **Acquire from Cloud**: Opens the Cloud Data Import Wizard, which allows you to pull data from Facebook, Google, or Twitter, provided you have authentication tokens, or the user's account credentials.

See Overview on page 123 for more information on evidence processing.

Setting Individual Case Options

Case Options are specific to individual cases. You select case options from the case Home page by clicking **Case** > **Options** or by selecting **Options** from the Case dropdown menu.



To configure case options, change the following options:

- **Primary evidence cache**: Use the browse button to change this folder to use the Primary evidence cache folder. This selection is disabled if you checked **Use base case folder for primary evidence cache** when first creating the case.
- **Secondary evidence cache**: If your case requires a second cache, use the browse button to change this folder to use the Secondary evidence cache folder.

To add or edit case information items, click the appropriate button on the **Case information** toolbar.

- **Split Mode**: Selects alternate views of the case information items.
- **Edit**: Edits case information items. Click the cell in the case information table whose information you want to change, then click **Edit** and modify the information.
- **New**: Adds a new blank row to the case information table at the current cursor position.
- **Delete**: Deletes case information items. Select the row to delete, then click **Delete**.

You cannot change the **Name** or the **Full case path**; these exist for informational purposes only.

Case Operations

Use the **Case** menu and the **Case** selections on the Case Home page to work with the parameters of and perform actions on your case.

The Case Selections table below shows a list of basic operations for working with a case. Use the menu items on the Case menu and the links beneath the Case section on the Case panel for these operations.

Case Selections

Save	Saves the current case file. The default file extension for a case file is Case. The default extension for a backup case file is cbak.
Save As Template...	Saves the case as an EnCase template to use with new cases. The file extension for a case template is CaseTemplate.
Create Package	Packages a case to share with other users or environments.
Case Backup	Creates a backup of the current case. Alternately, it allows you to specify a different case file or a case backup location.

Options...	Edits the case options for the active case.
Hash Libraries...	Displays the Hash Libraries dialog, which provides a list of hash libraries and hash sets used in the current case. Allows you to change libraries or enable and disable hash libraries and sets.
Close	Closes the active case file.
Open...	Opens an existing case file. Note that you can have more than one case file active at a time.
New Case...	Opens the Case Options dialog so you can create a new case file.

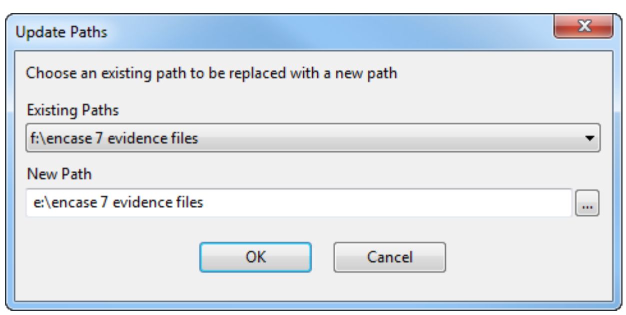
Changing the Evidence Path if the Evidence File is Moved

If you try to open a case where one or more of the evidence file locations has changed, a prompt displays indicating the evidence path could not be found.

Click **OK**. You can then reassociate the evidence to the new location when you drill into the evidence or view the evidence for the first time. Saving the case after that commits the change.

Alternatively, you can use the **Update Paths** button:

1. On the **Evidence** tab, click the checkbox for the evidence file where you want to change the path, then click **Update Paths**.
2. In the Update Paths dialog, choose an existing path from the dropdown menu.
3. In the New Path field, enter or browse to the new path.



4. Click **OK**.

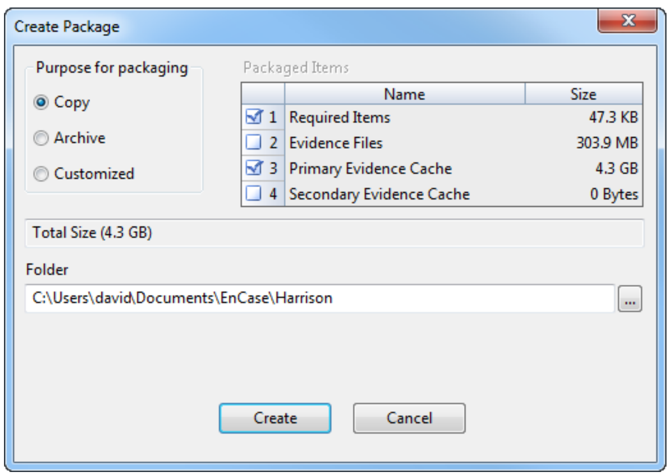
Case Portability

The Case Package option offers a convenient way of sharing entire cases among users, or porting a case to a different computer or environment.

An EnCase package can contain the entire contents of a case, including the evidence and cache files, or a subset of case-related items. You decide which case items to include when saving a case package.

To save a case as a package:

1. On the Home page, click **Case** > **Create Package**. The Create Package dialog displays.



2. The Create Package dialog offers several options for including case-related material in an EnCase case package:
   - The default **Copy** option (shown above) includes only the **Required Items** for the case file and the **Primary Evidence Cache**.
   - If you click the **Archive** option, all **Packaged Items** are automatically checked. Although you gain the advantage of packaging all evidence files and the secondary evidence cache, the package size can be extremely large.
   - If you click the **Customize** option, in the list of Packaged Items you can manually check any combination of packaged items you want to include in the case package.

3. Save the case package to a folder. Either use the default folder path or click the browse button to navigate to a different folder.

Case Page Logo

You can change the logo that is displayed on the right side of the Case page. From the right hamburger menu, select **Change Case Page Logo**. Navigate to your desired image and change the display size if desired.

CHAPTER 4

CASE BACKUP

Overview	91
Case Backup Dashboard	91
Settings and Options	92
Backing up a New Case	93
Viewing Case Backup Options	94
Creating a Scheduled Backup	94
Creating a Custom Backup	94
Deleting a Backup	95
Changing Case Backup Settings	95
Specifying a Case File	96
Specifying a Backup Location	97
Restoring a Case from Backup	97

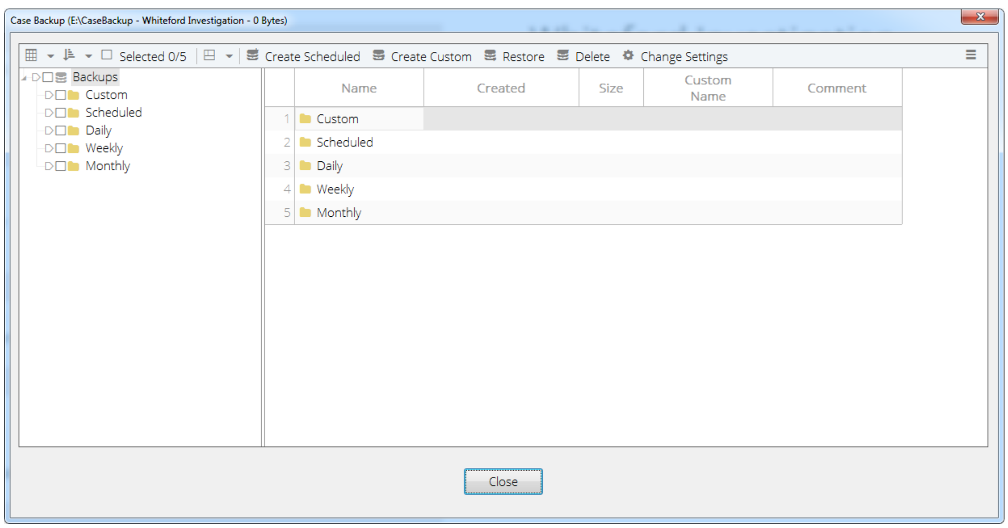
Overview

This chapter describes how to back up your cases and their related items, and how to restore a case from backup.

Case Backup Dashboard

The key interface for interacting with all backups for a particular case is the case backup dashboard. For each case backup, the dashboard displays:

- Name
- Created
- Size
- Custom Name (if available)
- Comment (if available)



The dashboard shows a list of all available case backups and sorts them by the following types:

- Custom: This is a user created backup where you can provide a custom name and comments. Custom backups are retained until explicitly deleted.
- Scheduled: A scheduled backup is created when you open a new case or schedule a backup manually using the **Create Scheduled** option.
- Daily: Every scheduled backup that is closest to that day's local midnight time is copied and stored as a daily backup.
- Weekly: Every daily backup that is closest to that week's Sunday local midnight time is copied and stored as a weekly backup.

- Monthly: Every daily backup that is closest to that month's first day at local midnight time of the next month is copied and stored as a monthly backup.

By default, the database stores a maximum of:

- 48 scheduled backups
- Seven daily backups
- Five weekly backups

Monthly backups are kept until the maximum size allowed is exceeded. The oldest monthly backups are deleted to stay under the maximum size allowed.

You can access the dashboard in three ways from the Case Backup option in the Case dropdown menu:

- **Use Current Case**: Uses the backup location from the currently open and active case.
- **Specify Case File**: Reads from and uses the backup location from an unopened case file through an open file dialog.
- **Specify Backup Location**: Uses the backup location specified by the user through a folder dialog.

Depending on how you access the dashboard, you can:

- Create a scheduled backup.
- Create a custom backup.
- Restore a case from backup.
- Delete one or more backups.
- Change case backup settings.

Settings and Options

Case backup settings are case-specific and stored in the case file itself. These settings are configurable at the time of case creation. Case backup dialogs contain:

- A checkbox to enable/disable backup every 30 minutes.
- A maximum amount of disk space (in GB) text box.
- A backup folder location text box.

When you create a new case, you can:

- Enable or disable backup every 30 minutes. The default is Enabled.
- Set the maximum case backup size (GB). The default is 50.

- Specify the backup folder location. The default is `User Directory\CaseBackup`.

The last backup folder location, maximum amount of disk space, and enable/disable backup are saved in the global settings and automatically populated when you create a new case.

When you first create a case, these constraints are checked:

- If you create a case with backup disabled, a dialog asks if you are sure you want to disable backup for this case.
- A warning displays if the backup location is not a valid path.
- Choosing a backup and case folder on the same drive letter displays a warning asking if you are sure you want to back up the case on the same drive as the case.
- Choosing a backup and evidence cache folder on the same drive letter displays a warning asking if you are sure you want to back up the case on the same drive as the evidence cache.

Note: It is good practice to have your backup in a different location from your current data.

Automatic Backup

Since backups can take a significant amount of time, they occur in a background thread, allowing you to continue with your work.

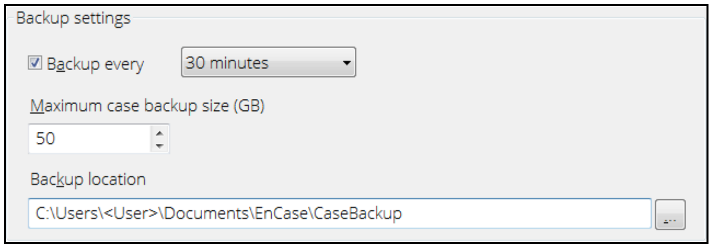
Automated backup every 30 minutes:

- Can be canceled at any time by double clicking the thread.
- Stops if the case is closed.
- If interrupted, continues at a later time, resuming where it left off.
- Stops if the Evidence Processor is running. This is because Evidence Processor creates and modifies a significant amount of data which is eventually backed up. Backing up files as they are being modified is not possible or desirable.
- Does not run if the Evidence Processor is already running.
- Disables the automated backup timer while running.

Backing up a New Case

To configure backup for a new case:

1. On the home page, click **New Case**.
2. The Options dialog displays. Enter needed information in the **Name and location** and **Evidence cache locations** areas.
3. Specify the backup settings you want.



- Select or clear the **Backup every 30 minutes** checkbox. The box is selected by default.
- Enter a **Maximum case backup size** (**GB**). The default is 50.
- Enter or browse to the **Backup location**.

4. Click **OK**.

Viewing Case Backup Options

After creating the case, you can view case backup settings in the case options dialog. Click **Case** > **Options** to view backup settings and other information.

To modify case backup options, click **Case** > **Case Backup** > **Use Current Case**. For more information, see Changing Case Backup Settings on the facing page.

Creating a Scheduled Backup

1. Click **Case** > **Case Backup** > **Use Current Case**. The dashboard displays.
2. Click **Create Scheduled**.
3. The Create Scheduled Backup dialog displays.
4. Click **OK**. The Created Scheduled Backup progress bar displays.
5. After the backup is scheduled, the Create Scheduled Backup dialog closes.

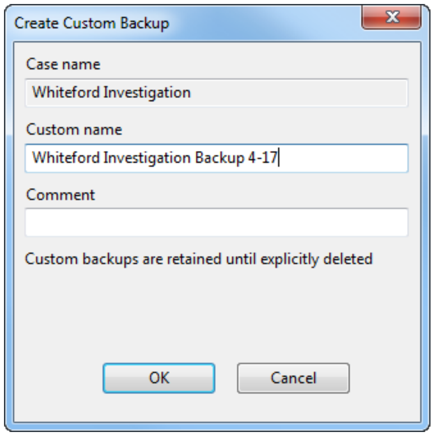
Creating a Custom Backup

Use custom backup to provide a custom name for the backup and to add optional comments.

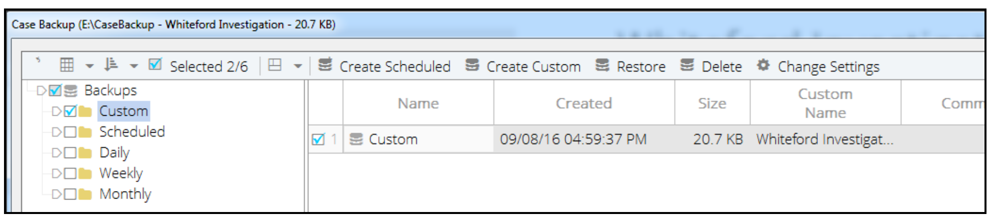
To create a custom backup:

1. Click **Case** > **Case Backup** > **Use Current Case**. The dashboard displays.
2. Click **Create Custom**.

3. The Create Custom Backup dialog displays.



4. Enter a custom name and, if desired, a comment, then click **OK**.
5. To verify the custom backup was created, click the **Custom** folder in the Backups directory.



Deleting a Backup

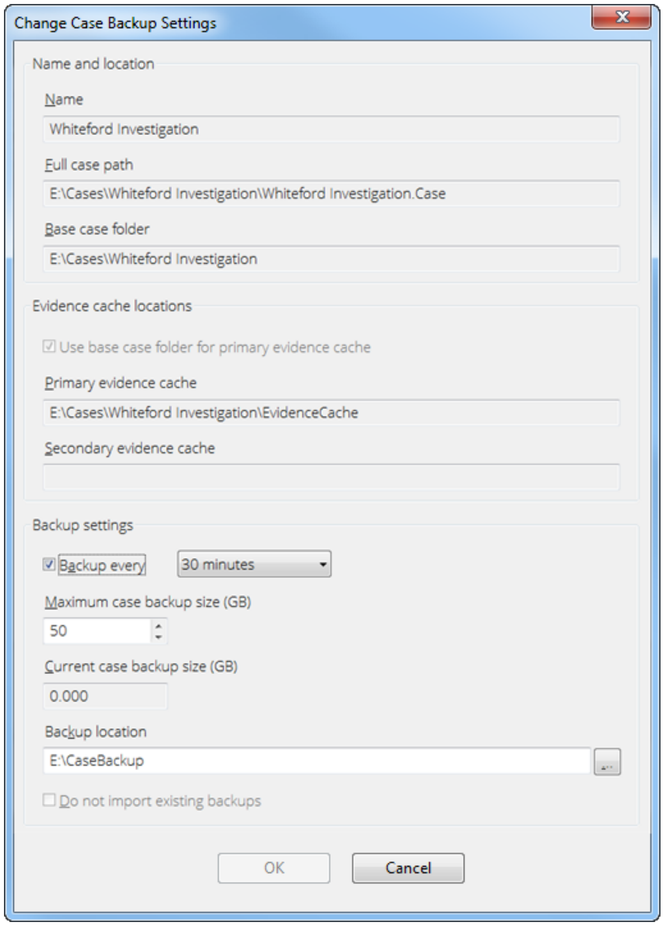
To delete a backup:

1. Go to the dashboard using any of the options in the **Case** > **Case Backup** dropdown menu. In the Backups directory, open the folder containing the backup you want to delete.
2. Blue check the backup or backups you want to delete, then click **Delete**.
3. A warning message displays.
4. To continue, click **OK**. The selected backups are deleted.

Changing Case Backup Settings

To change case backup settings:

1. Click **Case** > **Case Backup** > **Use Current Case**.
2. On the dashboard, click **Change Settings**.
3. The Change Case Backup Settings dialog displays.



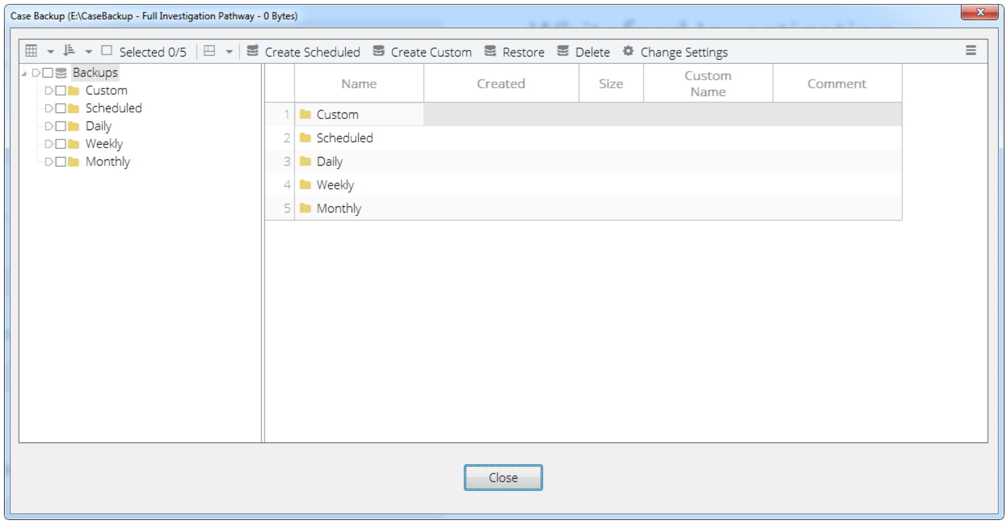
4. You can:
   - Enable or disable backup every 30 minutes.
   - Set the **Maximum case backup size (GB)**. If you enter a size below the current case backup size, monthly backups are deleted to get below the new value. If not enough monthly backups are deleted, scheduled backup no longer occurs.
   - Designate the backup location. Changing the backup location enables the **Do not import existing backups** checkbox, giving you the option not to migrate existing backups to the new location.

5. Make the changes you want, then click **OK**.

Specifying a Case File

Use **Specify Case File** to select and open a case other than the current case.

1. Click **Case** > **Case Backup** > **Specify Case File**. The Open File dialog displays.
2. Select the case file you want, then click **Open**. The dashboard displays for the case file you selected.



Specifying a Backup Location

To specify a backup location:

1. Click **Case** > **Case Backup** > **Specify Backup Location**. The Browse for Folder: Case Backup Location dialog displays.
2. Navigate to the location you want for the backup, then click **OK**.

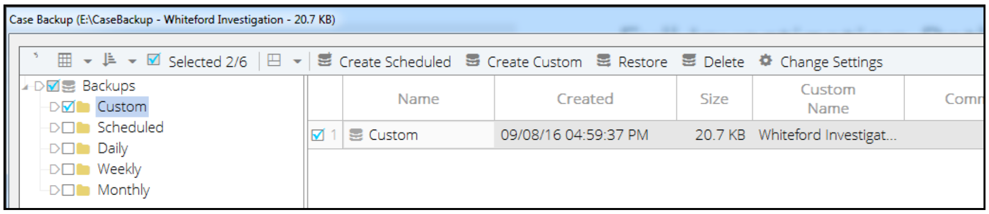
Restoring a Case from Backup

Restoring from backup restores these types of data:

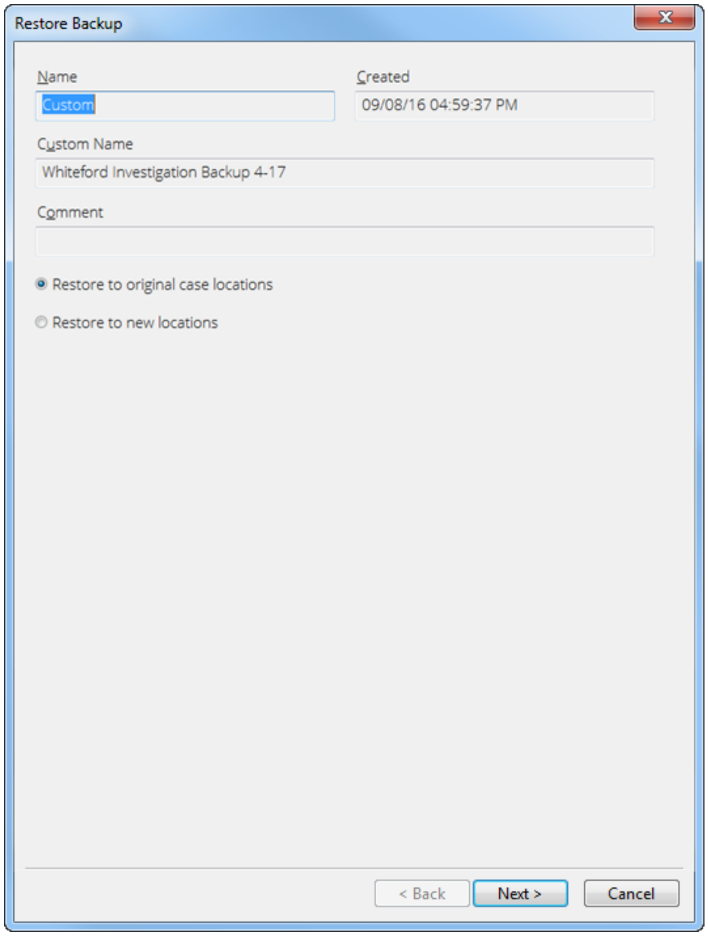
- Case file
- Everything in the case folder, except:
  - Export folder
  - Temp folder
  - Evidence files (.E01, .L01, .Ex01, and .Lx01)
- Primary evidence cache (only those evidence caches referenced in the case)
- Secondary evidence cache (only those evidence caches referenced in the case)
- Dates, times, and sizes for all files

To restore from backup:

1. Open EnCase.
2. At the top left of the screen, click **Case** > **Case Backup** > **Specify Backup Location**.
3. Browse to the folder containing the backups, then click **OK**.
4. Select the case name in the left pane and click **OK**.
5. In the dashboard, select the folder in the Backups directory containing the backup you want to restore.
6. Blue check a single backup, then click **Restore**.



7. The Restore Backup dialog displays. Click either **Restore to original case locations** (default) or **Restore to new locations**, then click **Next**.



- If you click **Restore to original case locations**, the Name, Location, and Full case path fields populate automatically and you cannot edit them. All other options are disabled.
- If you click **Restore to new locations**, the Name, Location, and Full case paths fields populate and you cannot edit them. However, all other options are enabled, and you can change any of them.

8. When you are done, click **Finish**.

Note: You cannot restore into the currently open case.

CHAPTER 5

ACQUIRING DEVICES AND EVIDENCE

Overview	103
Sources of Acquisitions	103
Canceling an Acquisition	104
Types of Evidence Files	104
Verifying Evidence Files	106
Acquiring a Local Drive	106
Audit Drive Space	107
Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA)	107
Using a Write Blocker	108
Acquiring a Disk Running in Direct ATA Mode	109
Acquiring Disk Configurations	110
Acquiring Other Types of Supported Evidence Files	115
CD-DVD Inspector File Support	115
Acquiring a DriveSpace Volume	116
Reacquiring Evidence	116
Adding Raw Image Files	117
Restoring a Drive	118

Overview

With EnCase, you can directly process and analyze storage device and evidence file previews with some limitations; however, if you want to use all of EnCase's processing and analysis features, you need to perform a storage device or evidence file acquisition and save the evidence in a standard format.

With EnCase, you can reacquire and translate raw evidence files into EnCase evidence files that include CRC block checks, hash values, compression, and encryption. You can also add EnCase evidence files created in other cases. EnCase can read from and write to current or legacy EnCase evidence files and EnCase logical evidence files.

With the LinEn utility, you can perform disk-to-disk acquisitions, and when you couple LinEn with EnCase, you can perform network crossover acquisitions.

This chapter provides detailed information about all types of EnCase acquisitions.

Sources of Acquisitions

EnCase can acquire the following sources:

- Previewed memory or local devices such as hard drives, memory cards, or flash drives.

  Note: It is not uncommon on live systems to have the on disk image of a file system to differ from its current state. In this event, Guidance Software recommends you flush the operating system disk cache using the **Sync** command.

- Evidence files supported by EnCase, including current EnCase evidence files (.Ex01), current logical evidence files (.Lx01), legacy EnCase evidence files (.E01), legacy logical evidence files (.L01).
- DD images, SafeBack images, VMware files (.vmdk), or Virtual PC files (.vhd). You can use these to create legacy EnCase evidence files and legacy logical evidence files, or you can reacquire them as EnCase .Ex01 or .Lx01 format, adding encryption, new hashing options, and improved compression.
- Single files dragged and dropped onto the EnCase user interface. These include ISO files, which create .L01 or .Lx01 logical evidence files.
- Mobile Devices, using the **Acquire from Device** selection in the **Acquire Mobile** menu.
- Mobile backup files, using the Acquire from File selection in the Acquire Mobile menu.
- Network crossover using LinEn and EnCase to create .E01 files or .L01 files. This strategy is useful when you want to preview a device without disassembling the host computer. This

is usually the case for a laptop, a machine running a RAID, or a machine running a device with no available supporting controller.

Sources for acquisitions outside EnCase include:

- LinEn for disk-to-disk acquisitions that do not require a hardware write blocker.
- WinEn for acquiring physical memory from a live Windows computer.
- Tableau Forensic Duplicators (TD1, TD2, and TD3).

Canceling an Acquisition

You can cancel an acquisition while it is running. After canceling, you can restart the acquisition.

To cancel an acquisition while it is running:

1. At the bottom right corner of the main window, double click the **Thread Status** line. The Thread Status dialog displays.
2. Click **Yes**. The acquisition is canceled. You can restart it at a later time.

You can also cancel remote acquisitions using the Remote Acquisition Monitor.
See Monitoring a Remote Acquisition on page 1.

Types of Evidence Files

EnCase Forensic supports the following evidence file types:

- EnCase evidence files (.E01 or .Ex01)
- Logical evidence files (.L01 or .Lx01)
- Raw Image files
- Single files

EnCase Evidence Files

The .Ex01 evidence file format supports LZ compression, AES256 encryption with keypairs or passwords, and options for MD5 hashing, SHA-1 hashing, or both. The .Ex01 evidence file format is not compatible with legacy versions of EnCase.

Legacy EnCase evidence files (.E01) are a byte-for-byte representation of a physical device or logical volume. You can create and save logical evidence files in the .L01 format in order to be compatible with legacy versions of EnCase (versions prior to EnCase 7). The .E01 format can be password protected.

EnCase evidence files provide forensic-level metadata, the device-level hash value, and the content of an acquired device.

Drag and drop an .E01 or .Ex01 file anywhere in the EnCase interface to add it to the currently opened case.

Logical Evidence Files

Logical evidence files can be saved in the .Lx01 file format. The .Lx01 file format supports LZ compression and options for MD5 hashing, SHA-1 hashing, or both.

Legacy logical evidence files (.L01) are created from previews, existing evidence files, or mobile device acquisitions. These are typically created after an analysis locates some files of interest. For forensic reasons, they are kept in a forensic container. Encryption is not available for legacy logical evidence files. You can create and save logical evidence files in the .L01 format in order to be compatible with legacy versions of EnCase (versions prior to EnCase 7).

When an .L01 or .Lx01 file is verified, the stored hash value is compared to the entry's current hash value.

- If the hash of the current content does not match the stored hash value, the hash is followed by an asterisk (*).
- If no content for the entry was stored upon file creation, but a hash was stored, the hash is not compared to the empty file hash.
- If no hash value was stored for the entry upon file creation, no comparison is done, and a new hash value does not populate.

Raw Image Files

Raw image files are a dump of the device or volume. There are no hash comparisons or CRC checks. Therefore, raw image files are not as forensically sound as EnCase image files. Although the files are not in EnCase format, EnCase supports a number of popular formats.

Before you can acquire raw image files, you must add them to a case. Raw image files are converted to EnCase evidence files during the acquisition process, adding CRC checks and hash values if selected.

Single Files

To add folders and single files to a case, either drag and drop them onto the EnCase interface using Windows Explorer, or using the Edit Single Files dialog. Once you add a file or folder to a case, the evidence page displays an item in the table for Single Files. Files and folders display in a tree structure subordinate to Single Files when displayed in the Entries view.

> **Note:** If you encounter difficulty adding single files from a mapped drive, try dragging and dropping the file from the UNC path.

Verifying Evidence Files

Verify Evidence Files checks CRC values of selected files. It is a way to ensure that evidence is not tampered with. Verified CRC information is written out to a log file. From the **Evidence** tab, you can check the **CRC Errors** tab in the bottom pane and bookmark any sectors that contain errors.

To perform an Evidence File verification:

1. Acquire the evidence files.
2. Add the evidence files to your case.
3. Click **Tools** > **Verify Evidence Files**.
4. The Verify Evidence Files dialog displays.
5. Select one or more evidence files, then click **Open**. During verification, a progress bar displays in the lower right corner of the window.

Acquiring a Local Drive

Before you begin, verify that the local drive to be acquired was added to the case.

1. To protect the local machine from changing the contents of the drive while its content is being acquired, use a write blocker. See Using a Write Blocker on page 108.
2. Verify that the device being acquired shows in the Tree pane or the Table pane as write protected.

Acquiring Non-local Drives

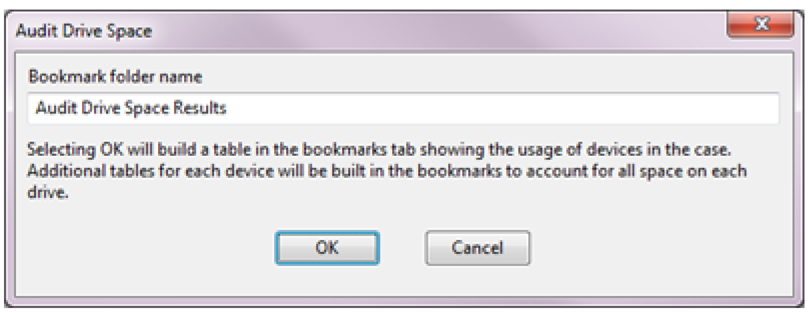
The LinEn utility acquires non-local drives by performing a network crossover acquisition. When you use the LinEn utility to acquire a disk through a disk-to-disk acquisition, you must add the resulting EnCase evidence file to the case using the Add Device wizard.

Audit Drive Space

To determine the amount of disk space available on a device, you can audit the space usage on that device.

To audit drive space:

1. On the home page in the Pathways group, click **Full Investigation**.
2. In the Let's get started group, click **Audit Drive Space**. The Audit Drive Space dialog displays.



3. Enter a bookmark folder name or accept the default, then click **OK**.

To view audit results:

1. Click on **View** > **Bookmarks** from the main menu.
2. Bookmarks display in the tree pane.
3. Click the Audit Drive Space Results bookmarks entry to display audit details in the table pane.

Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA)

EnCase applications can detect and image DCO and/or HPA areas on any ATA-6 or higher-level disk drive. These areas are detected using LinEn (Linux) or a Tableau write blocker. EnCase applications running in Windows with a hardware write blocker do not detect DCOs or HPAs.

This applies to EnCase applications using:

- Tableau
- LinEn when the Linux distribution used supports Direct ATA mode

The application shows if a DCO area exists in addition to the HPA area on a target drive.

HPA is a special area located at the end of a disk. It is usually configured so the casual observer cannot see it, and so it can be accessed only by reconfiguring the disk. HPA and DCO are extremely similar: the difference is the SET_MAX_ADDRESS bit setting that allows recovery of a removed HPA at reboot. When supported, EnCase applications see both areas if they coexist on a hard drive.

> **Note:** If you choose to remove a DCO, it will make a permanent change to the drive controller of the device.

Using a Write Blocker

Write blockers prevent inadvertent or intentional writes to an evidence disk. Their use is described in the following sections:

- Windows-based Acquisitions with Tableau and FastBloc Write Blockers below
- Acquiring in Windows using FastBloc SE on the facing page
- Acquiring in Windows without a Tableau or FastBloc Write Blocker on the facing page

Windows-based Acquisitions with Tableau and FastBloc Write Blockers

The following write blockers are supported in EnCase:

- Tableau T35es
- Tableau T35es-RW
- Tableau T4
- Tableau T6es
- Tableau T8-R2
- Tableau T9
- FastBloc FE
- FastBloc 2 FE v1
- FastBloc 2 FE v2
- FastBloc LE
- FastBloc 2 LE
- FastBloc 3 FE

Computer investigations require a fast, reliable means to acquire digital evidence. These are hardware write blocking devices that enable the safe acquisition of subject media in Windows to an EnCase evidence file. Before write blockers were developed, non-invasive acquisitions were exclusively conducted in cumbersome command line environments.

The hardware versions of these write blockers are not standalone products. When attached to a computer and a subject hard drive, a write blocker provides investigators with the ability to quickly and safely preview or acquire data in a Windows environment. The units are lightweight, self-contained, and portable for easy field acquisitions, with on-site verification immediately following the acquisition.

Support for Tableau write blocker devices enables EnCase to:

- Identify a device connected through the Tableau device as write blocked.
- Access the Host Protected Area (HPA) and access, via removing, the Device Configuration Overlay (DCO) area of a drive using the Tableau device.

> **Note:** EnCase does not support access of DCO areas via EnScript. By default, HPA is automatically disabled on the device.

Acquiring in Windows using FastBloc SE

Guidance Software includes the FastBloc SE module with EnCase. This is a software write blocker that can be applied to devices connected by USB, FireWire, or SCSI interfaces. For more information, see FastBloc SE on page 743.

Acquiring in Windows without a Tableau or FastBloc Write Blocker

Never acquire hard drives in Windows without a write blocker because Windows writes to any local hard drive visible to it. Windows will, for example, put a Recycle Bin file on every hard drive that it detects and will also change Last Accessed date and time stamps for those drives.

Media that Windows cannot write to are safe to acquire from within Windows, such as CD-ROMs, write protected floppy diskettes, and write protected USB thumb drives.

Acquiring a Disk Running in Direct ATA Mode

If the Linux distribution supports the ATA mode, you will see a **Mode** option. You must set the mode before acquiring the disk. An ATA disk can be acquired via the drive-to-drive method. The ATA mode is useful for cases when the evidence drive has a Host Protected Area (HPA) or

Drive Control Overlay (DCO). Only Direct ATA Mode can review and acquire these areas.

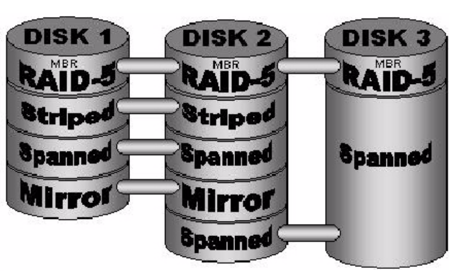
Ensure LinEn is configured as described in LinEn Setup Under SUSE on page 622, **autofs** is disabled (cleared), and Linux is running in Direct ATA Mode.

1. If the FAT32 storage partition to be acquired is not mounted, mount it.
2. Navigate to the folder where LinEn resides and enter `./linen` in the console.
3. The LinEn main screen displays.
4. Select **Mode**, then select **Direct ATA Mode**. You can now acquire the disk running in ATA mode.
5. Continue the drive-to-drive acquisition.

Acquiring Disk Configurations

Guidance Software uses the term disk configuration instead of RAID. A software disk configuration is controlled by the operating system software (or LVM software), whereas a controller card controls a hardware disk configuration. In a software disk configuration, information pertinent to the layout of the partitions across the disks is located in the registry or at the end of the disk, depending on the operating system. In a hardware disk configuration, it is stored in the BIOS of the controller card. With each of these methods, you can create six disk configuration types:

- Spanned
- Mirrored
- Striped
- RAID-5
- RAID-10
- Basic



Software RAID

EnCase applications support these software RAIDs:

- Windows NT: See Windows NT Software Disk Configurations below.
- Windows 2000: See Dynamic Disk on page 113.
- Windows XP: See Dynamic Disk on page 113.
- Windows 2003 Servers: See Dynamic Disk on page 113.
- Windows Vista: See Dynamic Disk on page 113.
- Windows Server 2008: See Dynamic Disk on page 113.
- Windows Server 2008R2: See Dynamic Disk on page 113.
- Windows 7: See Dynamic Disk on page 113.
- Windows 8: See Dynamic Disk on page 113.

RAID-10

RAID-10 arrays require at least four drives, implemented as a striped array of RAID-1 arrays.

Hardware Disk Configuration

Hardware disk configurations can be acquired:

- As one drive.
- As separate drives.

Windows NT Software Disk Configurations

In a Windows NT file system, you can use the operating system to create different types of disk configurations across multiple drives. The possible disk configurations are:

- Spanned
- Mirrored
- Striped
- RAID 5
- Basic

The information detailing the types of partitions and the specific layout across multiple disks is contained in the registry of the operating system. EnCase applications can read this registry information and resolve the configuration based on the key. The application can then virtually mount the software disk configuration in the EnCase case.

There are two ways to obtain the registry key:

- Acquiring the drive
- Backing up the drive

Acquire the drive containing the operating system. It is likely that this drive is part of the disk configuration set, but in the event it is not—such as the disk configuration being used for storage purposes only—acquire the OS drive and add it to the case along with the disk configuration set drives.

To make a backup disk on the subject machine, use Windows Disk Manager and select **Backup** from the **Partition** option.

This creates a backup disk of the disk configuration information, placing the backup on a CD or DVD. You can then copy the file into EnCase using the **Single Files** option, or you can acquire the CD or DVD and add it to the case. The case must have the disk configuration set drives added to it as well. This process works only if you are working with a restored clone of a subject computer. It is also possible a registry backup disk is at the location.

In the EnCase **Evidence** tab:

1. Select the device containing the registry or the backup disk and all devices which are members of the RAID.
2. Click the **Open** button to go to the Entry view of the **Evidence** tab.
3. Select the disk containing the registry, then click the dropdown menu on the upper right menu of the **Evidence** tab.
4. Select **Device**, then select **Scan Disk Configuration**.

At this point, the application attempts to build the virtual devices using information from the registry key.

Support for EXT4 Linux Software RAID Arrays

EnCase Forensic Imager provides the ability to parse EXT4 Linux Software RAID arrays (for Ubuntu version 9.1 and version 10.04), using the **Scan for LVM** option in the Device dropdown menu.

These configurations are supported:

- RAID 1 (mirror)
- RAID 10

> **Note:** EnCase Forensic Imager does not support partial reconstruction of RAIDs. After parsing, all RAID devices must have full descriptors or the process will fail.

Dynamic Disk

Dynamic Disk is a disk configuration available in Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server, Windows 7, Windows 8, and Windows 2008 Server R2. The information pertinent to building the configuration resides at the end of the disk rather than in a registry key. Therefore, each physical disk in this configuration contains the information necessary to reconstruct the original setup. EnCase applications read the Dynamic Disk partition structure and resolve the configurations based on the information extracted.

To rebuild a Dynamic Disk configuration:

1. Add the physical devices involved in the set to the case.
2. In the **Evidence** tab, select the devices involved in the Dynamic Disk.
3. Click the **Open** button on the menu bar to change to the Entries view of the **Evidenc**e tab.
4. Select the devices, then click the dropdown menu at the top right of the **Evidence** tab.
5. Select **Device** and choose **Scan Disk Configuration**.

If the resulting disk configurations seem incorrect, you can manually edit them:

1. Return to the highest Evidence view of the **Evidence** tab.
2. Select the **Disk Configuration** option.
3. Click the dropdown menu from the top right corner of the **Evidence** tab.
4. Select **Edit Disk Configuration**.

Disk Configuration Set Acquired as One Drive

Unlike software disk configurations, those controlled by hardware contain necessary configuration information in the card’s BIOS. Because the disk configuration is controlled by hardware, EnCase cannot reconstruct the configurations from the physical disks. However, since the pertinent information to rebuild the set is contained within the controller, the computer (with the controller card) actually sees a hardware disk configuration as one (virtual) drive, regardless of whether the set consists of two or more drives. Therefore, if the investigator acquires the set in its native environment, the disk configuration can be acquired as one drive, which is the easiest option. The best method for performing such an acquisition is to conduct a crossover network cable acquisition.

> **Note:** The LinEn boot disk for the subject computer needs to have Linux drivers for that particular RAID controller card.

To acquire the set:

1. Keep the disk configuration intact in its native environment.
2. Boot the subject computer with a Live Linux Boot Disk containing the LinEn utility and configured with the drivers for the RAID controller card.
3. Launch the LinEn utility.

   Note: The BIOS interprets the disk configuration as one drive, so EnCase applications will as well. The investigator sees the disk configuration as one drive.

4. Acquire the disk configuration as you normally acquire a single hard drive, depending on the means of acquisition. Crossover network cable or drive-to-drive acquisition is straight-forward, as long as the set is acquired as one drive.

If the physical drives were acquired separately, or could not be acquired in the native environment, EnCase applications can edit the hardware set manually.

Disk Configurations Acquired as Separate Drives

Sometimes acquiring the hardware disk configuration as one drive is not possible, or the method of assembling a software disk configuration seems incorrect. Editing a disk configuration requires this information:

- Stripe size
- Start sector
- Length per physical disk
- Whether the striping is right handed

You can collect this data from the BIOS of the controller card for a hardware set, or from the registry for software sets.

When a RAID-5 consists of three or more disks and one disk is missing or bad, the application can still rebuild the virtual disk using parity information from the other disks in the configuration, which is detected automatically during the reconstruction of hardware disk configurations using the **Scan Disk Configuration** command.

When rebuilding a RAID from the first two disks, results from validating parity are meaningless, because you create the parity to build the missing disk.

To acquire a disk configuration set as one disk:

1. Add the evidence files to one case.
2. On the **Evidence** tab, click the gear icon in the far right corner to display a dropdown menu, then click **Create Disk Configuration**.
3. The Disk Configuration dialog displays. Enter a name for your disk configuration. Click the appropriate disk configuration.
4. Right click the empty space under Component Devices and click **New**.
5. Enter the start sector and size of the selected disk configuration, select the drive image which belongs as the first element of the RAID, then click **OK**.
6. Repeat steps 4 and 5 for each additional element drive of the RAID in order.
7. Back at the main Disk Configuration screen, set the Stripe Size, select whether this is a Physical Disk Image, and whether it uses Right-Handed Striping.
8. Once you are sure the settings and order of the drives is correct, click **OK**. EnCase will generate a new item in your **Evidence** tab containing the RAID rebuilt to your specifications. You can acquire this new Disk Configuration to an EnCase Evidence file and process in the EnCase Evidence Processor just like a physical drive.

Acquiring Other Types of Supported Evidence Files

In addition to the native EnCase file formats, *.Ex01, *.E01, *.Lx01, and *.L01, EnCase supports SafeBack files (*.001), VMware files (*.vmdk), and Virtual PC files (*.vhd) directly. To add any of these types of evidence files:

1. Select **Add Evidence File** from the Add Evidence view of the **Home** tab, or click the **Add Evidence** dropdown menu while in the **Evidence** tab and select **Add Evidence File**.
2. The Add Evidence File Dialog displays. Use the dropdown menu at the bottom right corner of the dialog to change to the appropriate file extension for your evidence or choose the **All Evidence Files** option.
3. Navigate to the location of your evidence and select the first file of the evidence set as you would for EnCase evidence files, then click **Open**.

CD-DVD Inspector File Support

EnCase applications support viewing files created using CD/DVD Inspector, a third-party product. Treat these files as single files when adding them, as zip files, or as composite files when using the file viewer. Drag single files into the application.

Acquiring a DriveSpace Volume

DriveSpace volumes are only recognized as such after they are acquired and mounted into a case. On the storage computer, mount the DriveSpace file as a volume, then acquire it again to see the directory structure and files.

To acquire a DriveSpace volume:

1. A FAT16 partition must exist on the examiner machine where you will Copy/Unerase the DriveSpace volume. You can create a FAT16 partition only with a FAT16 operating system (such as Windows 95).
2. Run FDISK to create a partition, then exit, reboot, and format the FAT16 partition using format.exe.
3. Image the DriveSpace volume.
4. Add the evidence file to a new case and search for a file named DBLSPACE.000 or DRVSPACE.000.
5. Right click the file and copy/unerase it to the FAT16 partition on the storage computer.
6. In Windows 98, click **Start** > **All Programs** > **Accessories** > **System Tools** > **DriveSpace**.
7. Launch DriveSpace.
8. Select the FAT16 partition containing the compressed ".000" file.
9. Select **Advance Mount** > **DRVSPACE.000**, then click **OK**, noting the drive letter assigned to it. The Compressed Volume File (.000) from the previous drive is now seen as folders and files in a new logical volume.
10. Acquire this new volume.
11. Create the evidence file and add to your case. You can now view the compressed drive.

Reacquiring Evidence

When you have a raw evidence file generated outside an EnCase application, reacquiring it results in the creation of an EnCase evidence file containing the content of the raw evidence file and providing the opportunity to hash the evidence, add case metadata, and CRC block checks.

You can move EnCase evidence files into a case even if they were acquired elsewhere. Make sure all segments of the evidence file set are in the same folder. Using Windows Explorer, navigate to the location of the EnCase evidence files. Drag the first file of the set onto the open instance of EnCase and the remaining files will automatically be added, reassembling the evidence in your new case.

You may also want to reacquire an existing EnCase evidence file to change the compression settings or the file segment size.

Reacquiring Evidence Files

Start by adding the evidence file(s) to your case as previously described. You can reacquire evidence either from the **Evidence** tab or through the Evidence processor. To reacquire in the **Evidence** tab:

1. Select the items you want to reacquire.
2. Click the **Open** button to change to the Entries view of the **Evidence** tab.
3. Highlight the item you want to reacquire, click **Acquire** on the top menu, and select **Acquire** from the dropdown menu.
4. Complete the Acquire Device dialog as you would for previewed evidence.
5. You can repeat steps 3 and 4 for each device or volume you want to reacquire.

Retaining the GUID During Evidence Reacquisition

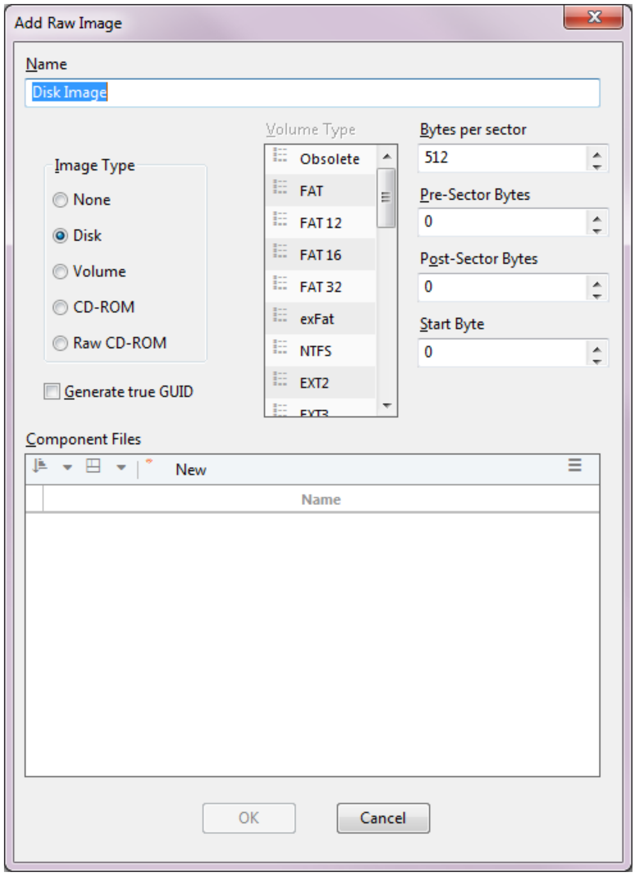
In the previous version of EnCase, the globally unique identifier (GUID) assigned to the evidence changed if the evidence was reacquired. EnCase now provides an option that retains the GUID when evidence is reacquired. To retain the GUID, select the **Keep GUID** checkbox that displays in the **Advanced** tab of the Acquire Device dialog. To open the Acquire Device dialog, select the device for acquisition in the Evidence Processor.

Adding Raw Image Files

Reacquiring raw evidence files like DD images or CD-ROM `.iso` files embeds the file containing the image of the device contents in an EnCase evidence file adding case metadata, CRC block checks and, optionally, the hash value of that image.

To acquire a raw evidence file:

1. In the **Add Evidence** dropdown menu, click **Add Raw Image**.
2. The Add Raw Image dialog opens.



3. Drag and drop the raw images to be acquired. The raw images to be added are listed in the Component Files list. For DD images or other raw images consisting of more than one segment, the segments must all be added in their exact order from first to last.
4. Click the **Generate true GUID** checkbox for EnCase to generate a unique GUID if a match is found.
5. Accept the defaults in the Add Raw Image dialog or change them as desired, then click **OK**.
6. A Disk Image object displays in the **Evidence** tab.
7. You can reacquire this image as you would any other supported evidence or previewed device.

Restoring a Drive

The following steps describe how to restore a drive.

Note: Before you begin, you first need to add evidence to the case.

1. From the EnCase top toolbar, select the **Evidence** option from the **View** dropdown.
2. In the Table view, click the evidence file with the device you want to restore.
3. From the **Device** dropdown on the **Evidence** tab menu, select **Restore**. The Restore dialog displays.
4. Click **Next** to collect local hard drives.
5. In the Local Devices list, click the drive you want to restore.
6. Click **Next**. The Drives dialog displays.
7. Select options for wiping and verification.
8. Click **Finish**.
9. A dialog displays asking you to verify the local drive selection. To verify you are restoring to the correct drive enter **Yes**, then click **OK**.

The bar in the lower right corner of the screen tracks the progress of the restore.

CHAPTER 6

PROCESSING EVIDENCE

Overview	123
Running Evidence Processor Options Incrementally	127
Conducting a Network Preview without a SAFE	129
Evidence Processor Prioritization	133
Evidence Processor Settings	134
Recovering Folders	135
Analyzing Protected Files	135
Analyzing Hashes	136
Analyzing Entropy Values	136
Analyzing File Signatures	138
Expanding Compound Files	138
Finding Email	139
Finding Internet Artifacts	139
Searching With Keywords	143
Creating an Index	148
Creating Thumbnails	153
Running EnScript Modules	153
Result Set Processing	162
EnScript Application UI	165
Processor Manager	166
Acquiring and Processing Live Previews	191

Overview

This chapter provides detailed information on the Evidence Processor, which processes evidence files in a large production environment. As a standalone product, the Evidence Processor is referred to as the EnCase Processor, which, aside from some licensing and set up differences (EnCase Processor-specific dongle), functions in exactly the same way as the Evidence Processor. Rather than installing separate instances of EnCase to perform processing only on multiple machines, you can install separate EnCase Processors and dongles instead for a fraction of the cost of a full EnCase license. For information on installing the EnCase Processor, see Installing and Configuring EnCase. All references to the Evidence Processor apply to EnCase Processor.

The Evidence Processor lets you run, in a single automated session, a collection of potent analytic tools against your case data. It can optimize the order and combinations of processing operations while running this multi-threaded process.

The Evidence Processor runs unattended. As it works in the background, you can continue to work with your case. The output of the Evidence Processor is stored on disk rather than memory for each device, so you can process multiple devices across several computers simultaneously. You can then bring all evidence back together into a case with no commingling of evidence data. By storing cache files on disk, you can scale to much larger data sets. As you reopen cases, you do not need to wait for data to resolve.

Run the Evidence Processor after you:

1. Review your evidence.
2. Add your evidence to a case.
3. Validate the data for browsing.
4. Set the time zones.

If you worked with a previous version of EnCase, you can continue to work cases using the methodology you developed for that previous version.

The Evidence Processor provides these features:

- Acquiring devices directly from the Evidence Processor.
- Processing a local without first acquiring a device.
- Saving sets of Evidence Processor options as templates. You can run these later with minimal modification.
- Guiding you through the use of each setting with embedded assistance.

- Processing results automatically from any current EnScript module according to the current processor settings (Index, Keyword search, etc.).
- Rerunning previously created options on updated data when additional evidence becomes available.

The Evidence Processor also includes these functions:

- Folder recovery
- Hash analysis
- Compound file expansion
- Email search
- Internet artifact search
- Keyword search
- Index creation (not available for local previews)
- EnScript Module execution:
  - Parsing system information
  - Instant messaging
  - File carving
  - OtherEnScript modules

The Evidence Processor also provides options to run:

- File signature analysis (not available for local previews)
- Protected file analysis

Before you use the Evidence Processor, consider the following:

- Your case must contain evidence to process.
- The device you want to process is properly configured and ready.
  - RAID and LVM configurations are included.
  - Whole-disk encryption is removed.
  - Hidden partitions are added.

- If you are previewing a local or network device, you can run most Evidence Processor options before you acquire it. Text indexing is not available from a preview. To run all Evidence Processor options, you must acquire the device.
- Guidance Software recommends installing 64-bit EnCase whenever possible. Large files may cause the 32-bit version of EnCase Evidence Processor to run out of memory.
- Confirm that time zone settings are configured properly. Note that if no time zone is set for the evidence, EnCase uses the time zone setting of the examiner workstation. For more information, see Configuring Time Zone Settings on page 46.

After you add evidence to your case and configure the time zone settings:

1. Acquire the evidence. For more information, see Acquiring with the Evidence Processor on page 1.
2. Select the evidence you want to run through the Evidence Processor.

The lower left pane of the Evidence Processor window contains a table with these elements:

- A toolbar for managing Evidence Processor tasks and modules.
- A list of Evidence Processor tasks you can run. This includes a collection of EnScript modules.
- A checkbox that allows you to enable or disable each processing task.

Use this pane for choosing tasks and configuring settings. The Evidence Processor retains previously run settings.

File and edit settings for the Evidence Processor selections pane are located in its toolbar.

Setting	Description
Split Mode	Change the display format of the options pane.
Edit	Edit the options for a selected task in the window.
Save Settings	Save the current selection of settings as an Evidence Processor template.
Load Settings	Load a saved template to run against the current data.
Use Defaults	Select the checkboxes for these default options: • Recover folders • File signature analysis • Protected file analysis • Thumbnail creation • Hash analysis • Expand compound links • Find email • Index text and metadata
Options menu	Perform actions such as printing the results and changing the layout of the Evidence Processor panes.

To select an option, select its checkbox in the **Enabled** column.

- If a task name is listed in blue, click the name to begin configuring the task.
- If a task name is listed in black, no further configuration options are available for that task.

Setting	Description
Split Mode	Change the display format of the options pane.
Edit	Edit the options for a selected task in the window.
Save Settings	Save the current selection of settings as an Evidence Processor template.
Load Settings	Load a saved template to run against the current data.
Use Defaults	Select the checkboxes for these default options: • Recover folders • File signature analysis • Protected file analysis • Thumbnail creation • Hash analysis • Expand compound links • Find email • Index text and metadata
Hamburger menu	Perform actions such as printing the results and changing the layout of the Evidence Processor panes.

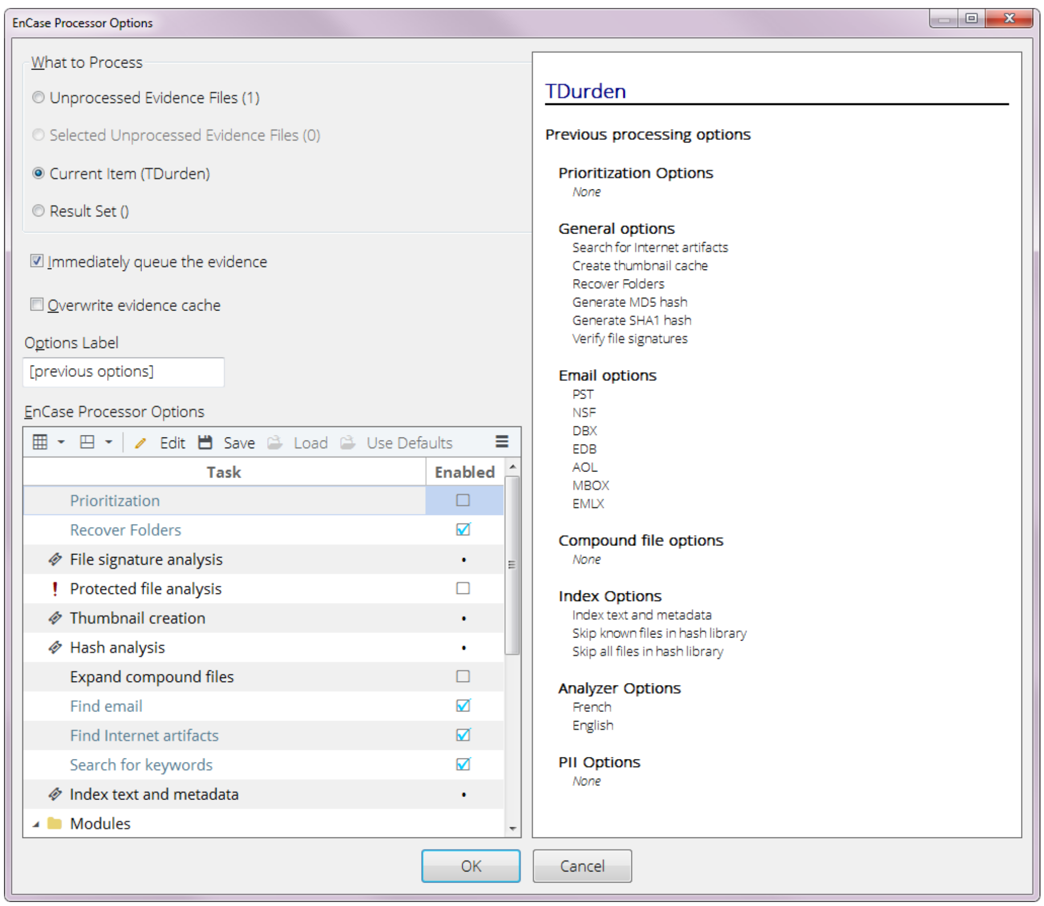
To select an option, select its checkbox in the **Enabled** column.

- If a task name is listed in blue, click the name to begin configuring the task.
- If a task name is listed in black, no further configuration options are available for that task.

Running Evidence Processor Options Incrementally

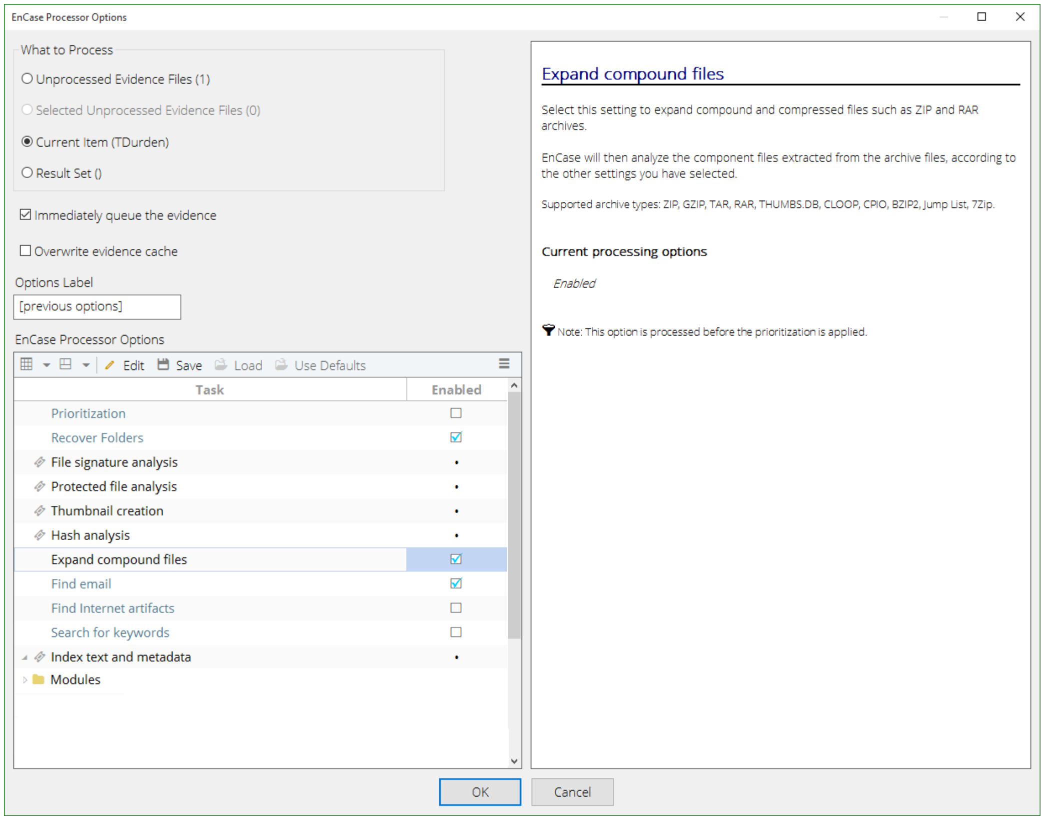
You can add options in the Evidence Processor as you continue an investigation. For example, you may want to run certain options in the beginning, such as file signature and hash analysis, then later add other options, such as parsing compound files. You can select additional options on subsequent Evidence Processor runs; however, you cannot remove previously run options.

When you select **Process** for an already processed item, the right pane of the EnCase Processor Options dialog displays previous processing settings.

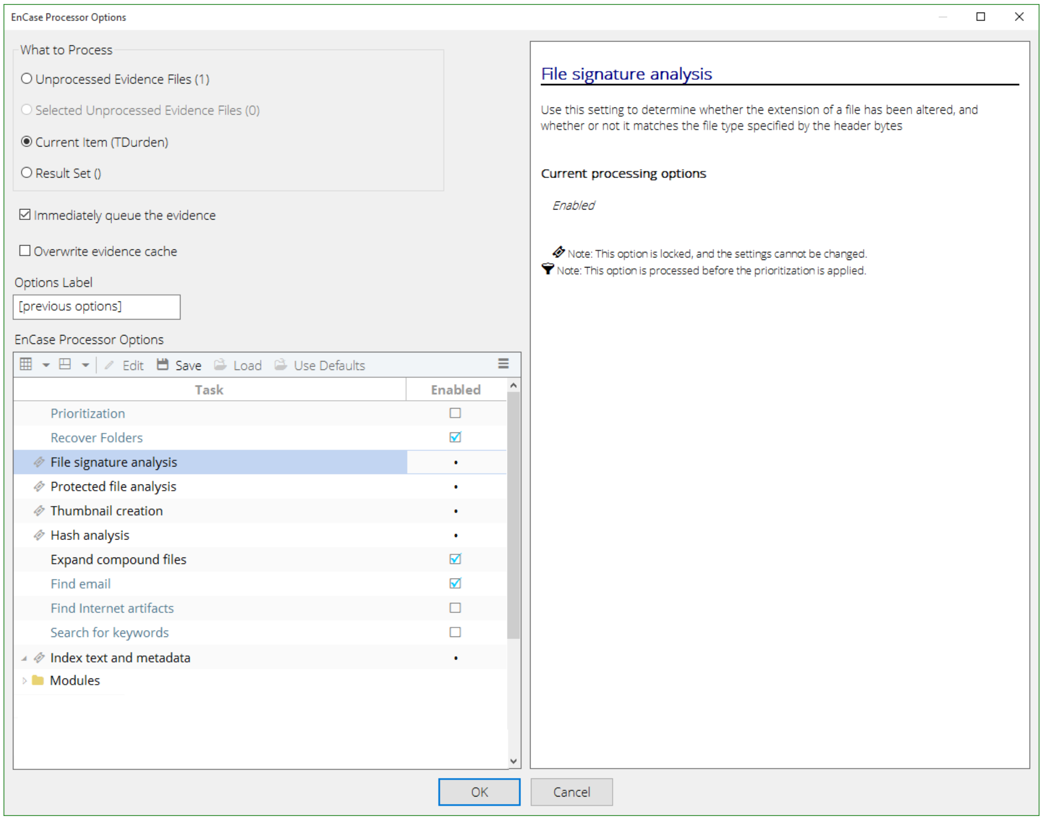


You can run modules over and over again with different settings each time. The results of each run are added to the case.

Clicking an option displays information about that option in the right pane.



Clicking an option with a lock icon displays the settings for that option.



Conducting a Network Preview without a SAFE

Direct Network Preview enables you to create agents and installers and conduct a network preview of an endpoint without using a SAFE.

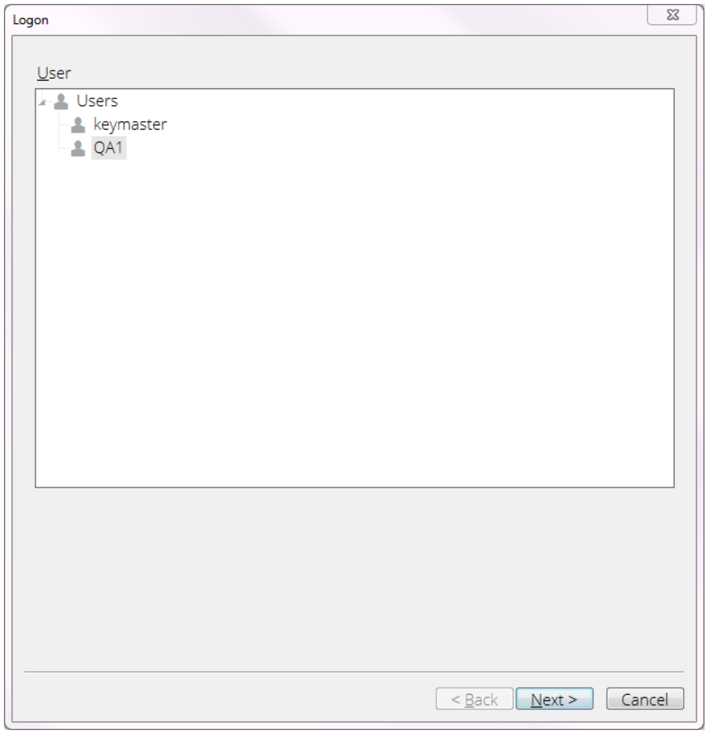
> **Note:** Direct Network Preview allows only one connection at a time.

Creating Direct Agents

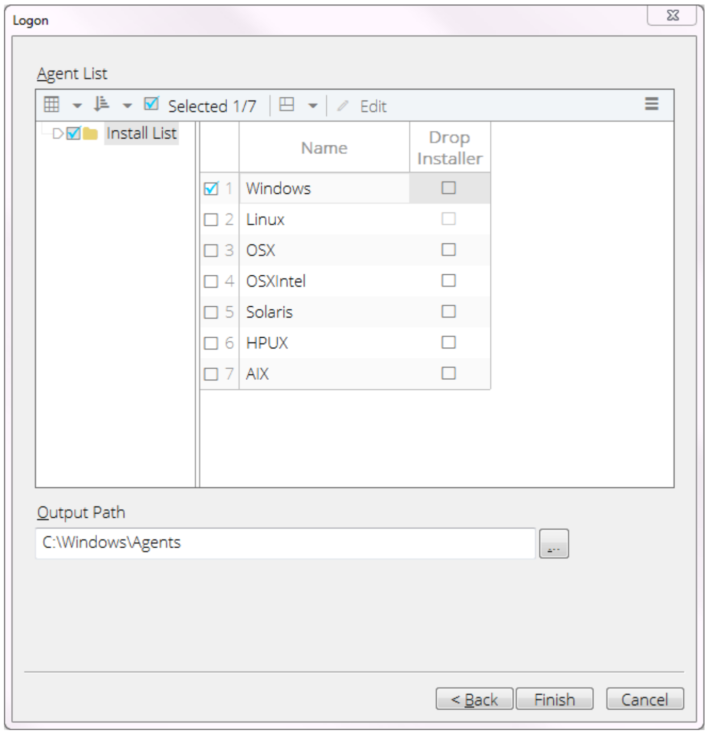
To create a direct network preview agent:

1. Click **Tools** > **Create Direct Agent**.
2. The Logon dialog displays. Select the public key you want to insert into the agent, then click **Next**.

> **Note:** If the desired public key does not display, right click in the dialog and select **Change Root Path**, then browse to the location containing the public key you want to use.



3. The next Logon dialog displays.

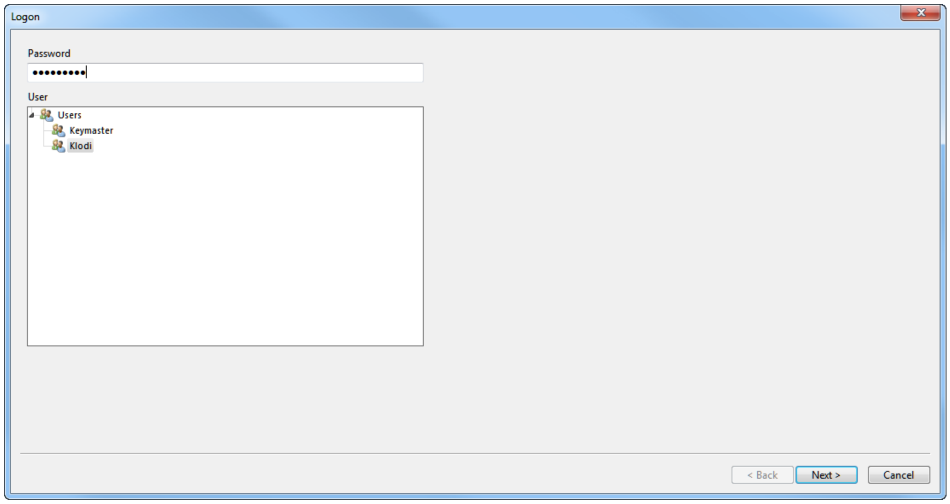


4. In the Agent List area, select the operating systems you want to create agents for.
5. Select drop installers, if desired.
6. Enter an output path or browse to the destination folder you want to use.
7. Click **Finish**. A status bar displays indicating the progress of the agent creation. When agent creation is complete, the dialog closes.

Adding a Direct Network Preview Device

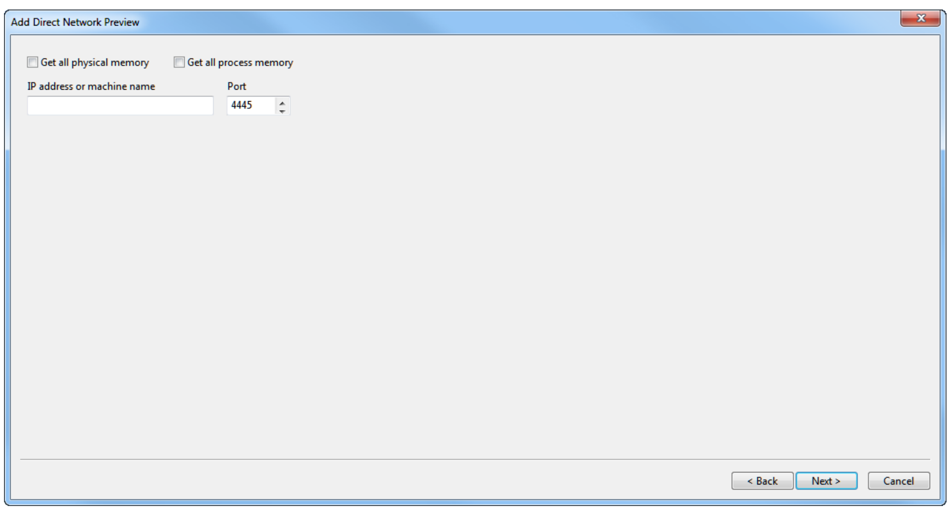
To add a direct network preview device:

1. Click **Add Evidence** > **Add Network Preview** > **Add Direct Network Preview**.
2. The Logon dialog displays.



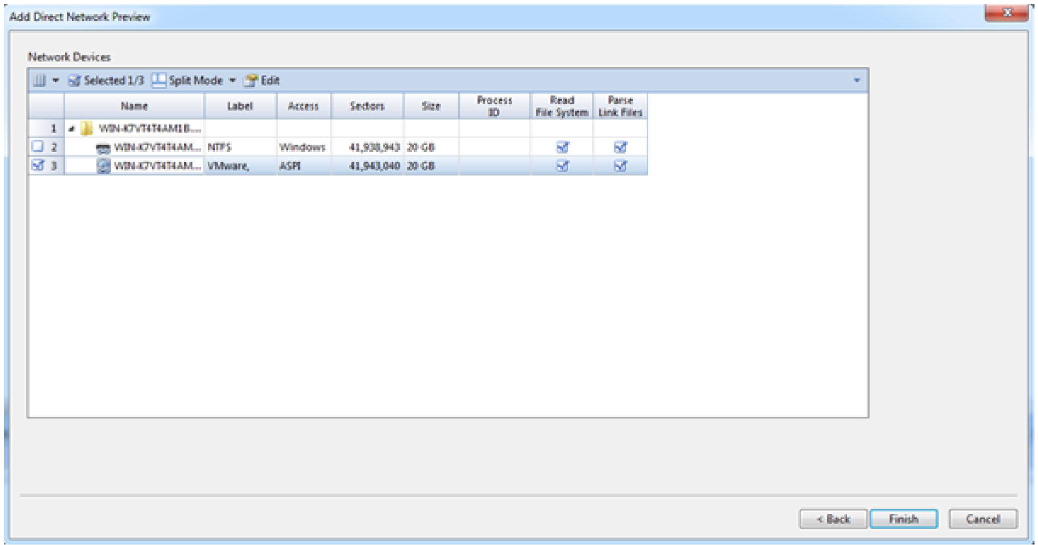
3. Select the key you used to create the agents, enter the password, then click **Next**. The Add Direct Network Preview dialog displays.

   Note: If the desired public key does not display, right click in the dialog and select **Change Root Path**, then browse to the location containing the public key you want to use.



   - **Get all physical memory** enables the acquisition of the target's RAM.
   - **Get all process memory** breaks up the memory usage by process. Process memory is what the process currently has stored in RAM.

4. Enter an IP address or machine name and select a port number, then click **Next**.



5. Select the device you want to add to the evidence image table, then click **Finish**.

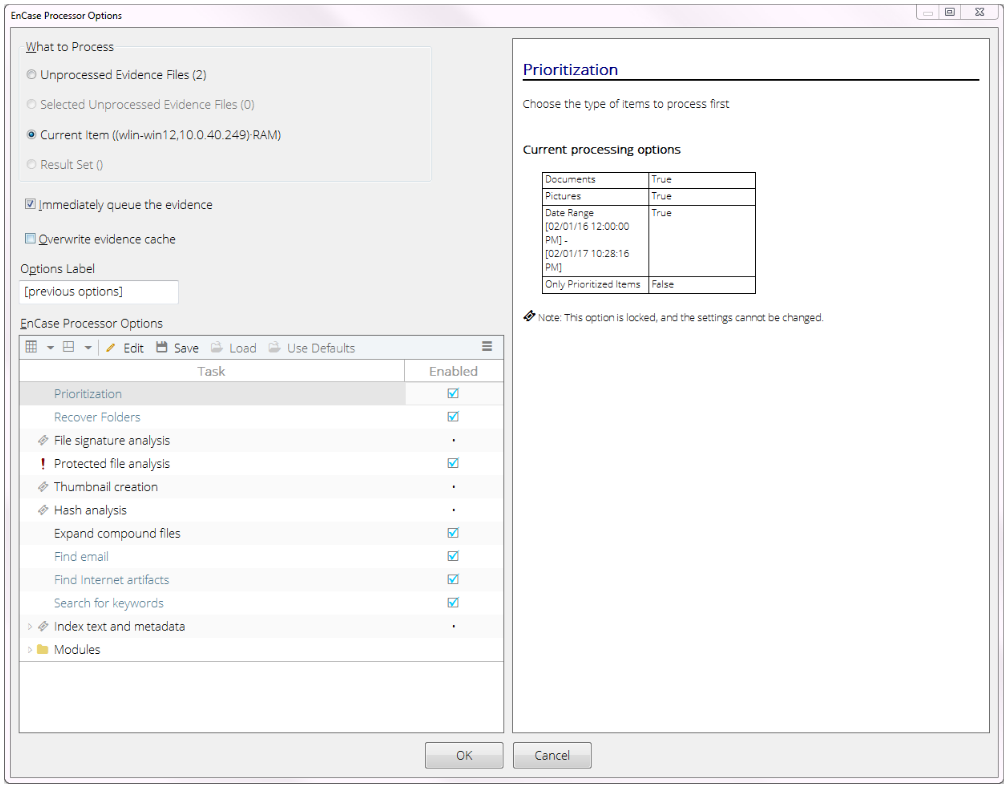
Evidence Processor Prioritization

The Evidence Processor enables you to process a subset of the evidence and begin examining it while the Evidence Processor continues to process the remaining evidence.

1. Select evidence to process. The EnCase Processor Options dialog displays.
2. Click the **Prioritization** option. The Processing Prioritization dialog displays.
3. Click the checkboxes (**Documents**, **Pictures**, or **Items within these dates**) for the items you want to have priority in processing. You can select more than one checkbox. Checking **Items within these dates** enables the **Minimum Date** and **Maximum Date** fields. You can enter dates and times manually or use the calendar (for dates). If you want to change a time, edit it manually.
4. If you want to process only the types of items you selected, instead of all evidence in the evidence image, click the **Process only prioritized items** checkbox.

   Note: If you select **Process only prioritized items**, you cannot run any Evidence Processor modules.

5. When you are finished, click **OK**. The EnCase Processor Options dialog right pane reflects the prioritization selections you made.



6. Click **OK** to begin processing the evidence.

Evidence Processor Settings

The Evidence Processor employs lock mechanisms that prevent you from configuring it in ways that create inconsistent states of evidence. These mechanisms allow flexibility when initially processing and reprocessing evidence.

The Evidence Processor also gives you the following options to designate only that evidence which you specifically want processed:

- During first time processing you can turn File Signature Analysis on or off. The default is on.

  Note: If you disable File Signature Analysis, after processing, images will not display in Gallery view.

- While reprocessing evidence:
  - You can turn Keyword Search on or off.
  - You can turn on Recover Folders if it was previously turned off.

Recovering Folders

Running the Recover Folders task on FAT partitions searches through the unallocated clusters of a specific FAT partition for the “dot, double-dot” signature of a deleted folder. When the signature matches, EnCase can rebuild files and folders that were in the deleted folder.

This task can recover NTFS files and folders from Unallocated Clusters and continue to parse through the current Master File Table (MFT) artifacts for files without parent folders. This operation is particularly useful when a drive was reformatted or the MFT is corrupted. Recovered files are placed in the gray Recovered Folders virtual folder in the root of the NTFS partition.

RECOVER FOLDER STRUCTURE OF NTFS 3.0 FILES OPTION

When you turn on the **Recover folder structure of NTFS 3.0 files** option, a heuristical algorithm attempts to reconstruct the original folder structure of recovered folders from an NTFS 3.0 operating system. If there are many recovered folders, this algorithm can take a long time to complete. When this option is off, all found recovered folders are grouped together, without a tree structure.

Analyzing Protected Files

Encrypted and password-protected files are identified, since you may need further investigation to process these files. The Evidence Processor's protected file analysis uses Passware's toolkit to identify the protected files. The strength of protection is stored so that you can first try to decrypt weaker passwords before applying them to more complex protection.

Because this process requires significant processing resources, process time may be unacceptably long. If this process is not critical for your analysis, you can disable it.

> **Note:** New encryption products and uncommon encryption products may not be detected.

Analyzing Hashes

A hash is a digital fingerprint of a file or collection of data, commonly represented as a string of binary data written in hexadecimal notation. In EnCase, it is the result of a hash function run against any mounted drive, partition, file, or chunk of data. The most common uses for hashes are to:

- Identify when a chunk of data changes, which often indicates evidence tampering.
- Verify that data has not changed, in which case the hash should be the same both before and after verification.
- Compare a hash value against a library of known good and bad hashes, seeking a match.

The Evidence Processor's hash analysis setting allows you to create MD5 and SHA-1 hash values for files, so you can use them later for the reasons described above. When you click the **Hash Analysis** hyperlinked name, the Edit Settings dialog displays, allowing you to check whether to run either or both of these hashing algorithms.

Analyzing Entropy Values

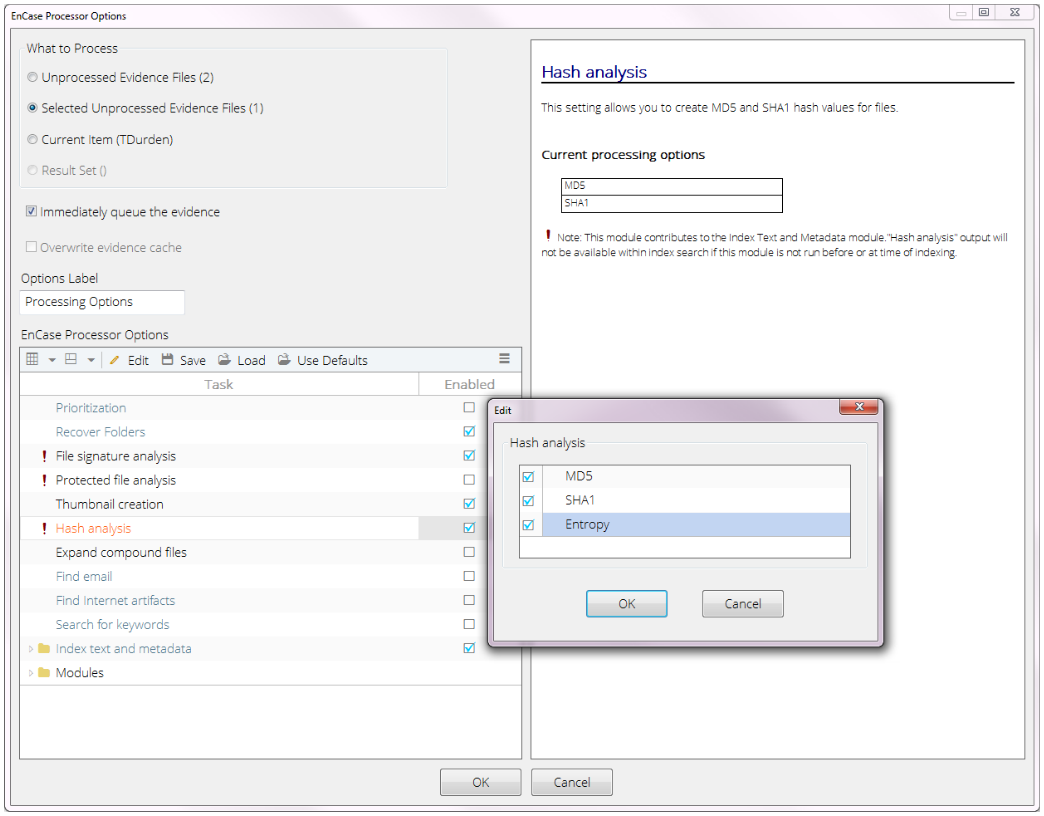
EnCase calculates entropy values for files. Entropy values show the degree of randomness of bytes in a file. These values can identify files that may be similar, and allow you to see files grouped according to their entropy values. Entropy values can assist you in finding encrypted or compressed files.

Entropy values range from 0 to 8. Values at the lower end of the range reflect less randomness; values at the higher end reflect greater randomness. Entropy values generated by EnCase are displayed in a column in Table view. Each entropy value consists of eight digits, for example 3.1577005.

Entropy analysis can be performed on an entire evidence set using Evidence Processor or on selected files by running **Hash\Sig Selected**.

To obtain entropy values with Evidence Processor:

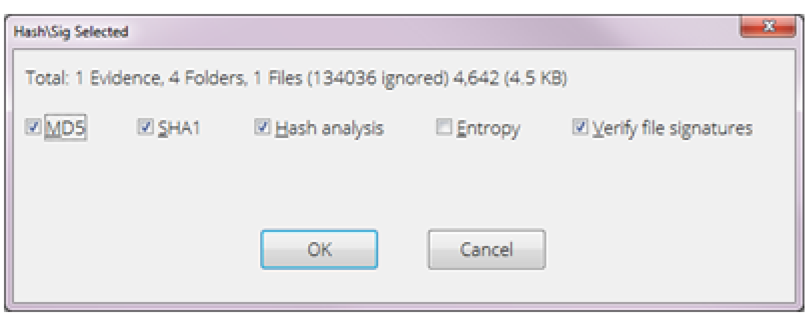
1. From the Process Evidence dropdown menu, select **Process**.
2. The EnCase Processor Options dialog displays. Click **Hash analysis**. The Edit hash analysis options dialog displays.



3. Click the Entropy checkbox and click **OK**.
4. When evidence processing completes, open the Evidence view and drill into the evidence.

To obtain entropy values for selected files and folders:

1. Check the folders containing the files for which you want to generate entropy values, then right-click on a selected item to display the context menu. Select **Entries** > **Hash\Sig Selected**.
2. The Hash\Sig Selected dialog displays.



- **MD5** generates MD5 hash values for the selected files.

- **SHA1** generates SHA1 hash values for the selected files.
- **Hash analysis** compares the hash values of selected files against hashes in your library.
- **Entropy** creates entropy values for the selected files.
- **Verify file signatures** performs file signature analysis on the selected files.

3. Click the **Entropy** checkbox and click **OK**.
4. You must leave Evidence view and reopen it to see the results in the Entropy column.
5. Table view displays resulting entropy values. Entropy numbers are highlighted to assist you in determining their significance in the result set.
   - If entropy equals 2, two numbers highlight in gray.
   - If entropy equals 5, five numbers highlight in gray.
   - If entropy equals 7, seven numbers highlight in gray.
   - If entropy equals 8, the entire entropy value is highlighted.

Analyzing File Signatures

A common technique for masking data is to rename a file and change its extension. For example, image files might be renamed so they look like dynamic-link library files. Signature analysis verifies file type by comparing the file headers, or signature, with the file extension.

File extensions are the characters following the dot in a file name (for example, signature.txt). They indicate the file's data type. For example, a .txt extension indicates a text file, and a .bmp extension indicates a bitmap image file. Standardized file types have unique signature-extension associations. For example, BM is the file signature for all .bmp files.

The signature analysis process flags all files with signature-extension mismatches according to its File Types tables. To view the Evidence Processor File Types table, click the **View** menu of the **Home** page and select **File Types**. For more information, see Adding and Modifying File Signature Associations on page 265. Signature analysis is always enabled so that it can support other Evidence Processor operations.

Expanding Compound Files

Use this setting to expand archive files, including .zip and .rar files.

For archive files, EnCase extracts the compressed or archived files and processes them according to the other Evidence Processor settings you chose. This includes nested archive files or zip files within a zip file. Note that EnCase handles compound document types like Microsoft Office Word separately.

Finding Email

Select this setting to extract individual messages and attachments from email archives. **Find Email** supports the following email types:

- PST (Microsoft Outlook)
- NSF (Lotus Notes)
- DBX (Microsoft Outlook Express)
- EDB (Microsoft Exchange)
- EMLX (Macintosh OS X)
- AOL
- MBOX

Note: EnCase blocks MBOX files from displaying in the **Doc** tab.

This setting prepares email archives for the use of email threading and related EnCase email functionality during case analysis.

To select which email archive types to search:

1. Click **Find Email**.
2. Click the email archive file types whose messages you want to examine, and click **OK**.

After processing completes, EnCase can analyze the messages and component files extracted from the email archives, according to the other Evidence Processor settings you selected.

HANDLING EMAIL ATTACHMENTS

When EnCase finds an attachment to an email message, it displays an attachment paper clip icon on top of the message icon. However, when email systems append a plain text version of the email together with the HTML/rich text version (this text is called an "alternate body"), EnCase displays a standard email icon. This occurs only when the alternate body is the only attachment to the email message.

Finding Internet Artifacts

Choose this Evidence Processor setting to find Internet-related artifacts, such as browser histories and cached web pages. The only setting that you can configure for Find Internet Artifacts is whether to search within unallocated space.

Currently, six browsers and two types of Internet history are supported. They are:

- Internet Explorer: History and cache
- Macintosh Internet Explorer: History and cache
- Safari: History and cache
- Firefox: History and cache
- Opera: History and cache
- Google Chrome:
    - History: A list of websites recently visited. This typically consists of websites, usage, and time related data.
    - Cookies: A list of recent authentication and session data for sites with persistent usage. This typically consists of website, expiration times, and site specific cookie data.
    - Cache: A list of recently cached files.
    - Downloads: A list of recently downloaded files. This typically consists of websites, file names, location, size, and date.
    - Keyword Search: A list of recent keyword searches. This typically consists of search terms and the search result page.
    - Login Data: A list of login data. This typically consists of websites, username, password, and SSL information.
    - Top Sites: A list of top websites. This typically consists of website information, rank, thumbnails, and redirect information.

Note: EnCase does not provide the ability to recover Google Chrome Internet artifacts from unallocated clusters.

Note: The difference between a regular search and a search of unallocated is that keywords are added internally and marked with a special tag indicating that it is for Internet history searching only.

Firefox Artifacts

As an enhancement to the Search for Internet history function, EnCase parses Firefox artifacts stored in a SQLite database and displays them in the **Artifacts** tab.

The types of Firefox 3 artifacts parsed are:

- Cookies
- Downloads
- History

- Bookmarks
- Form data

> **Note:** The **Artifacts** tab of an Internet history search for Mozilla Firefox artifacts displays **Frecency** and **Rev Host Name** columns.

"Frecency" is a valid word used by Mozilla. Do not mistake it for "frequency." For more information, see the Mozilla developer center article at https://developer.mozilla.org/en-US/docs/Mozilla/Tech/Places/Frecency_algorithm.

The value displayed in the **Frecency** column is the score Mozilla gives to each URL. It includes how frequently a person visits the site and how recently the user visits the site. EnCase displays this value as it is stored in the places.sqlite file.

Mozilla stores a URL's host name in reverse. EnCase displays it as such in the **Rev Host Name** column.



Frecency	Icon Url	Rev Host Name
100	http://www.google...	moc.elgoog.www.
100	http://www.google...	moc.elgoog.www.
100		moc.elgoog.www.
200	http://reviews.cnet...	moc.tenc.sweiver.
100	http://www.google...	moc.elgoog.www.

Safari Artifacts

OVERVIEW

Safari Versions 5 and 6 store Internet artifacts as:

- Cookies: stored as binary files.
- Cache: stored in a SQLite database.

> **Note:** Safari Version 6 stores some fields in binary plist format.

This browser software identifies artifacts using the Find Internet Artifacts module.

BINARY COOKIE PARSER

Safari uses a binary file to store cookies called "Cookies.binarycookies" with a "cook" file signature, using a proprietary format from Apple, NSHTTPCookieStorage.

Available fields include:

- URL Name
- URL Host

- Expiration Date
- Resource Path
- Content Identifier
- Created Date
- Title/Name

CACHE DATABASE PARSER

Safari uses a SQLite database to store cache (Cache.db). Every database version can be detected with cfurl_cache_schema_version. Some Safari Version 10 and 12 fields are stored as binary plist files.

Available fields include:

- Version
- Safari Hash Value
- Storage Policy
- URL Name
- URL Host
- Request Object
- Last Modification Time
- Response Object
- Accept Ranges
- Cache Control
- Connection
- Creation Date
- Content Length
- Content Type
- Internet Artifact Type
- Expiration
- Server
- Vary
- Browser Type
- Message Size
- Via
- Requesting URL
- Referrer
- Origin

Searching With Keywords

Keywords are text strings or search expressions created to find matching text within entries in a body of evidence. A search expression can be a GREP expression, containing variables, and it can be flagged to be case sensitive, a whole word search, or other options. You can also associate a particular codepage to use with a keyword. Codepages are alphabet sets of a variety of Latin and non-Latin character sets such as Arabic, Cyrillic, and Thai.

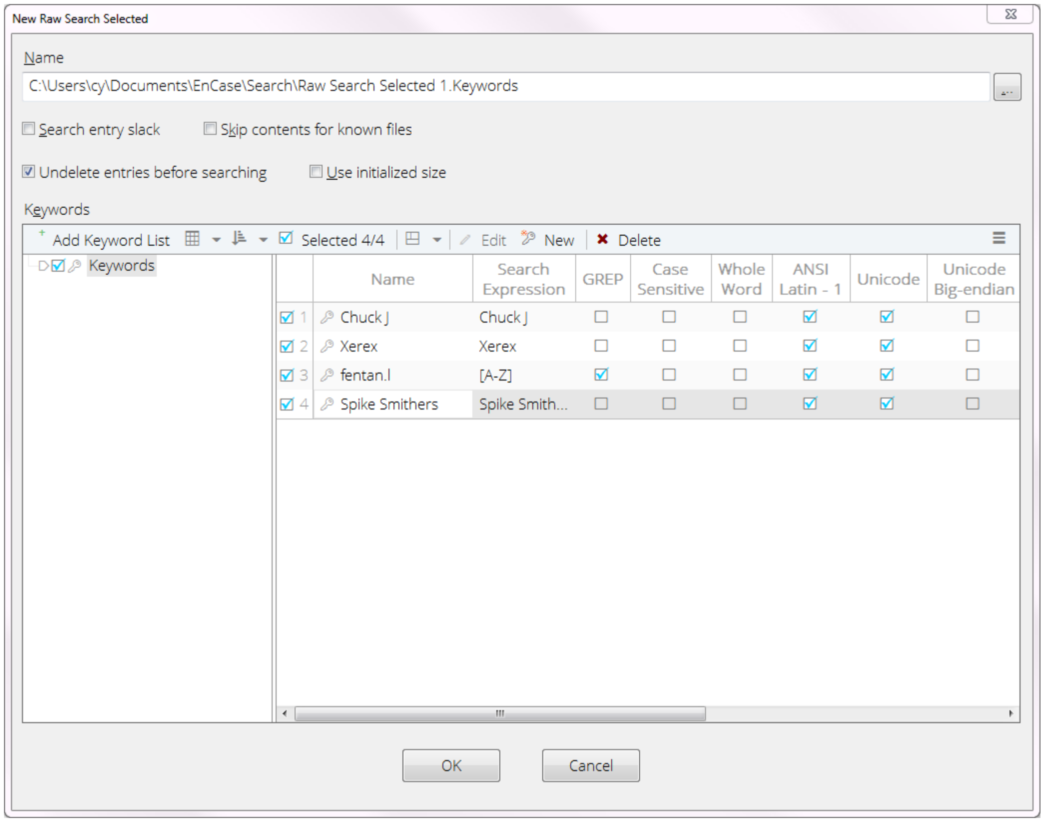
Note that if you are searching for a number and an application stores the number in a different format, EnCase will not find it. For example, in Excel, if a Social Security number is entered without dashes as 612029229, Excel stores it in double precision 64-bit format as 00008096693DC241.

Often, examiners have ready-made lists of keywords to use in their searches. You may also want to add additional keywords to use in your searches.

You can create and run keyword searches in several ways:

- With the Evidence Processor
  - Keyword searches created and conducted with the Evidence Processor are stored with the device's evidence cache files and can be used with any number of cases.
  - Keyword searches not initiated from the Evidence Processor are stored with the case and are case specific.
- By clicking **Raw Search All** on the Evidence Tab when viewing evidence. This is the best way to search through raw, non-indexed data.
- By clicking **Raw Search** when viewing entries.
  - The targeted search only acts on items selected in the current view.
  - To run a targeted search against two or more devices in your case, click **Open** in the **Evidence** tab and select additional devices.

Wherever you access it, the Keyword list displays a list of existing keywords in the case:



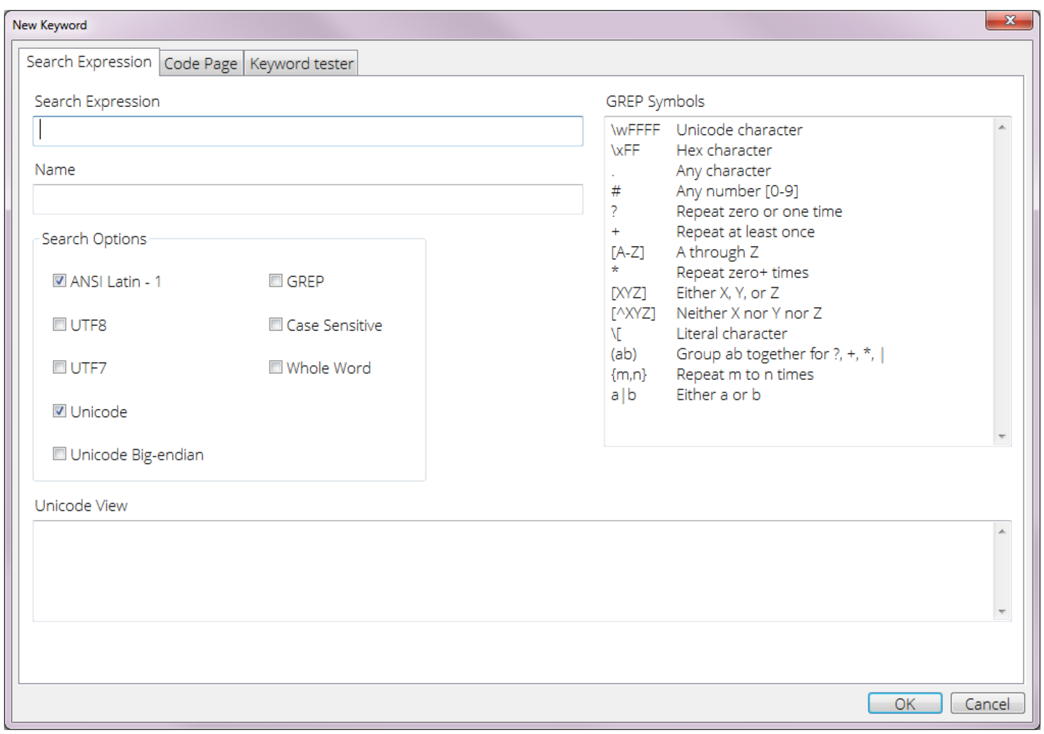
- Select **Search entry slack** to include file slack in the keyword search.
- **Use initialized size** enables you to search a file as the operating system displays it, rather than searching its full logical size.
  - In NTFS file systems, applications are allowed to reserve disk space for future operations. The application sets the logical size of the file larger than currently necessary to allow for expected future expansion, while setting the Initialized Size smaller so that it only needs to parse a smaller amount of data. This enables the file to load faster.
  - If a file has an initialized size less than the logical size, the OS shows the data area between the initialized size and logical size as zeros. In actuality, this area of the file may contain remnants of previous files, similar to file slack. By default, EnCase displays, searches, and exports the area past the initialized size as it appears on the disk, not as the OS displays it. This enables you to find file remnants in this area.
  - Select **Initialized Size** to see a file as its application sees it and the OS displays it.
  - Note that when a file is hashed in EnCase, the initialized size is used. This means that the entire logical file is hashed, but the area past the initialized size is set to zeros.

Since this is how a normal application sees the file, this enables users to verify file hashes with another utility that reads the file via the OS.

- Select **Undelete entries before searching** to undelete deleted files before they are searched for keywords.
- Select **Skip contents for known files** to only search the slack areas of known files identified by a hash library.
- **Add Keyword List** opens a dialog where you can enter a list of words and assign certain properties to them as a group. See Creating a New Keyword List on page 147.
- Double click a keyword, or click **Edit**, to open the keyword so you can modify its properties.
- Highlight a keyword and click **Delete** to remove it from the list.
- If a path box displays at the top of the dialog, that path and name is where the search is stored.

Adding a New Keyword

1. Select any option from the Raw Search menu to open the Raw Search dialog, which shows keyword lists.
2. In the Keyword toolbar, click **New**. The New Keyword dialog displays.



3. Enter the search expression and name, and select the desired options:

- **Search Expression** is the actual text being searched. Use a character map to create a non-English search string if your keyboard is not mapped to the appropriate non-English key mapping.
- **Name** is the search expression name listed in the folder.
- **ANSI Latin - 1** searches documents using the ANSI Latin - 1 code page.
- **UTF-8** meets the requirements of byte-oriented and ASCII-based systems. UTF-8 is defined by the Unicode Standard. Each character is represented in UTF-8 as a sequence of up to four bytes, where the first byte indicates the number of bytes to follow in a multi-byte sequence.

  Note: UTF-8 is commonly used in Internet and web transmission.

- **UTF-7** encodes the full BMP repertoire using only octets with the high-order bit clear (7 bit US-ASCII values, [US-ASCII]). It is deemed a mail-safe encoding.

  Note: UTF-7 is mostly obsolete, and is used when searching older Internet content.

- **Unicode:** select if you are searching a Unicode encoded file. Unicode uses 16 bits to represent each character. Unicode on Intel-based PCs is referred to as **Little Endian**. The Unicode option searches the keywords that display in Unicode format only. For more details on Unicode, see http://www.unicode.org.

  Note: The Unicode standard attempts to provide a unique encoding number for every character, regardless of platform, computer program, or language.

- **Unicode Big-endian:** select if you are investigating a big-endian Unicode operating system (such as a Motorola-based Macintosh). Big-endian Unicode uses the non-Intel data formatting scheme. Big- endian operating systems address data by the most significant numbers first.
- **GREP** uses GREP syntax (displayed on the right) for the search.
- **Case Sensitive** searches the keyword only in the exact case specified.
- **Whole Word** searches for whole keywords only.

4. Open the **Code Page** tab to change the code page to use a different character set.
5. To test a search string against a known file, click the **Keyword Tester** tab.

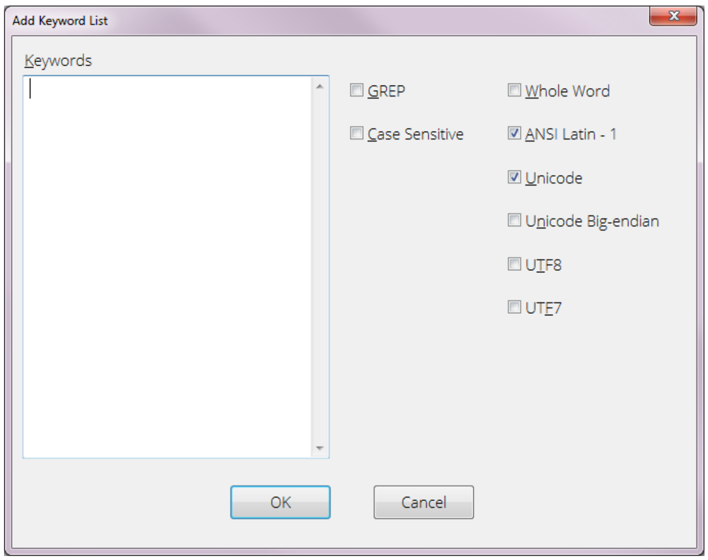
   - Locate a test file containing the search string, enter the address into the Test Data field, and click **Load.** The test file is searched and displays in the lower tab of the Keyword Tester form.
   - Hits are highlighted in both Text view and Hex view.

5. When you finish, click **OK**.

Creating a New Keyword List

When accessing the Keyword list from the Evidence tab by clicking **Raw Search All**, or when selecting options for a Keyword search, you have the option to create a keyword list.

1. From either location, from the New Keyword dialog click **Add Keyword List**. The Add Keyword List dialog displays.



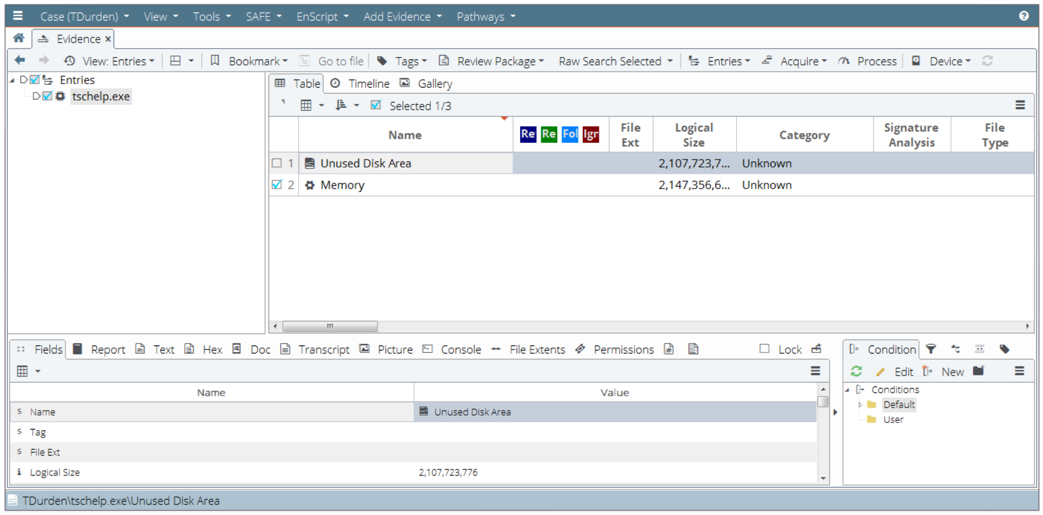
2. Add the keywords you want to use, one per line.
3. Select options to apply to all keywords from the checkboxes on the left. Individual words can have their options modified separately by editing them in the New Keyword dialog.
4. When you finish, click **OK**. The list populates the Keyword list and is saved in the path defined at the top of that dialog.

Searching for Keywords in Process Memory

1. Click **Add Evidence** > **Add Local Device**. The Add Local Device dialog displays.
2. Select **Enable Process Memory** and click **Next**.
3. Select the process you want to search for keywords, and click **Finish**.

   Note: Do not use **Raw Search All** for process memory searches because if the process is very large (for example, 8 TB) the keyword search takes a very long time.

4. Drill down in the process and select the **Memory** entry in the Table pane, then use **Raw Search Selected** to search for keywords.



Note: Because of the time it takes to search for 64-bit processes, Guidance Software recommends not searching through **Unused Disk Area**.

Creating an Index

Using the Evidence Processor to index your data enables you to search across all types of information and view results in email, files, mobile devices, and any other processed data in one search results view. All files, emails, and module output can be indexed, including EnScript modules such as the System Info Parser.

Generating an index can take time. Once generated, however, searching content becomes nearly instantaneous. Guidance Software recommends always indexing your case data.

Indexing Text in Slack and Unallocated Space

You can index text in file slack and unallocated space by selecting the **Index slack and unallocated** option when processing evidence.

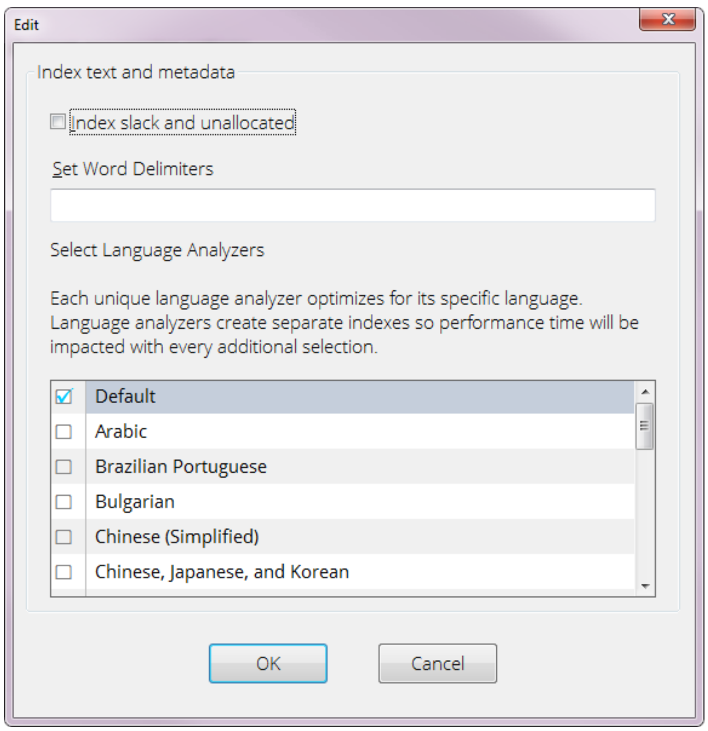
- **File slack**: the area between the end of a file and the end of the last cluster used by that file.
- **Unallocated space**: the sectors not associated with an allocated file: the free space of a disk or volume.
    - Unallocated space consists of either unwritten-to sectors or previously written-to sectors that no longer have historical attribution data associated with them. All

these sectors are aggregated into Unallocated Clusters.

- Unallocated Clusters are then divided into multiple sections, and these sections are indexed with shared metadata. If a word at the end of one section of text spans to another section of text, that word is skipped and not included in the indexed sections of text.
- Sectors not assigned to any partition fall under Unused Disk Area. The Evidence Processor handles these sectors and Unallocated Clusters similarly.

To index slack and unallocated space:

1. From the Evidence tab, select the evidence you want to process and select **Process Evidence** > **Process** from the menu bar. The EnCase Processor Options dialog displays.
2. Select the Index text and metadata checkbox to enable indexing, then click the **Index text and metadata** link. The Edit dialog displays.



3. Select **Index slack and unallocated**.
4. Click **OK**.

Setting Word Delimiters for Indexing

Add Word Delimiters to Search Index

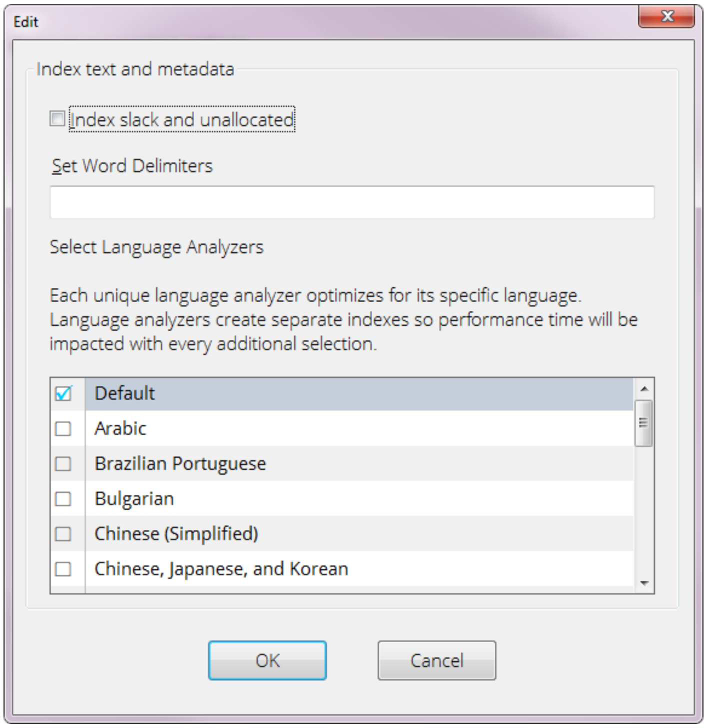
You can add word delimiters to your search index in addition to the default delimiters used with each language analyzer. Word delimiters are used to identify breaks between words in indexed data. Each Language analyzer has one or more standard delimiters it uses by default. There is no need to enter a delimiter if the language you are indexing uses that delimiter by default.

The indexing engine in EnCase Forensic uses the following delimiters for all analyzers by default. There is no need to add a delimiter if it is in this list.

```
!#$%&()*+,-\/;<=>?@[]^`{|}~
```

To add word delimiters for indexing:

1. From the Evidence tab, select the evidence you want to process, then select **Process Evidence** > **Process** from the menu bar of the Evidence tab. The EnCase Processor Options dialog displays.
2. Click the **Index text and metadata** link to display the Edit Index text and metadata dialog.
3. Enter one or more word delimiters without spaces in the text box.



4. Click **OK**.

Once your evidence is processed, all data will be indexed with the default word delimiters for the language analyzer as well as any additional delimiters added during processing. Any additional word delimiters entered during processing can be viewed by right-clicking on **Index text and metadata** link in the EnCase Processor Options dialog. The table that displays lists all current processing options.

Selecting a Language Index

EnCase Forensic uses language analyzers to index words for specific languages. Multiple analyzers can be chosen.

The English language analyzer is selected by default. It is optimized for the English language but indexes other Western languages as well.

Select other language analyzers to create an index for that language or language group. If you need to index and search evidence in a specific language, select the corresponding language analyzer to create a unique index for that language.

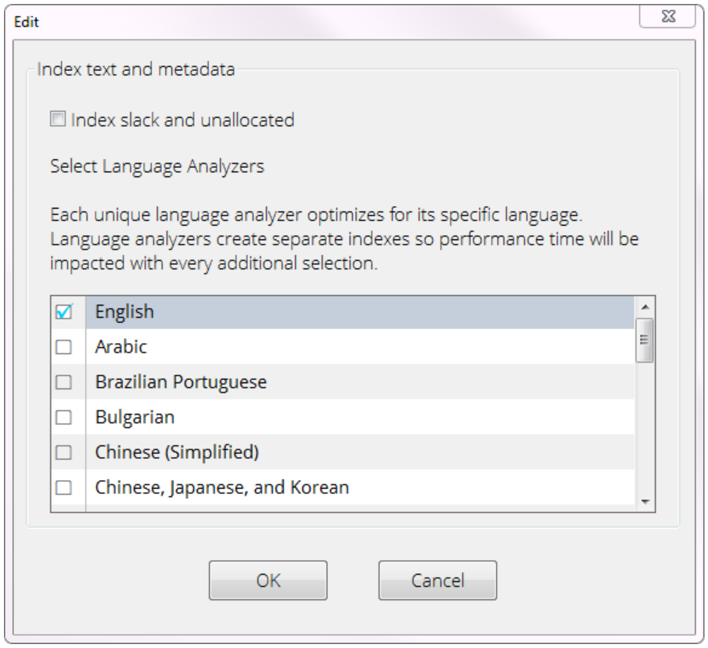
EnCase Forensic creates an index for each language you select. Indexing additional languages increases the time it takes to process your evidence. Guidance Software recommends selecting only the languages needed for your investigation.

You can create indexes in the following languages:

- English
- Arabic
- Brazilian Portuguese
- Bulgarian
- Chinese (Simplified)
- Chinese, Japanese, and Korean
- Danish
- Dutch
- Finnish
- French
- German
- Greek
- Hindi
- Italian
- Norwegian
- Romanian
- Russian
- Spanish
- Swedish
- Turkish

To create indexes for more than one language, or to change the default language index:

1. From the Evidence tab, select the evidence you want to process, then select **Process Evidence** > **Process** from the menu bar of the Evidence tab. The EnCase Processor Options dialog displays.
2. Select the Index text and metadata checkbox, then click the **Index text and metadata** link. The Edit dialog displays.



3. Select one or more languages you want to index.
4. Click **OK**.

Creating Thumbnails

When you select the Thumbnail creation option, the Evidence Processor creates thumbnail artifacts for all image files in the selected evidence. This facilitates image browsing.

Running EnScript Modules

EnCase Evidence Processor can run add-in modules (EnScript packages) during evidence processing. Modules are listed under **EnCase Processor Options** > **Modules**. Several modules are included with EnCase. You can also add your own EnScript packages. For examples of custom modules, open the C:\Program Files\EnCase8\EnScript\EvidenceProcessor folder.

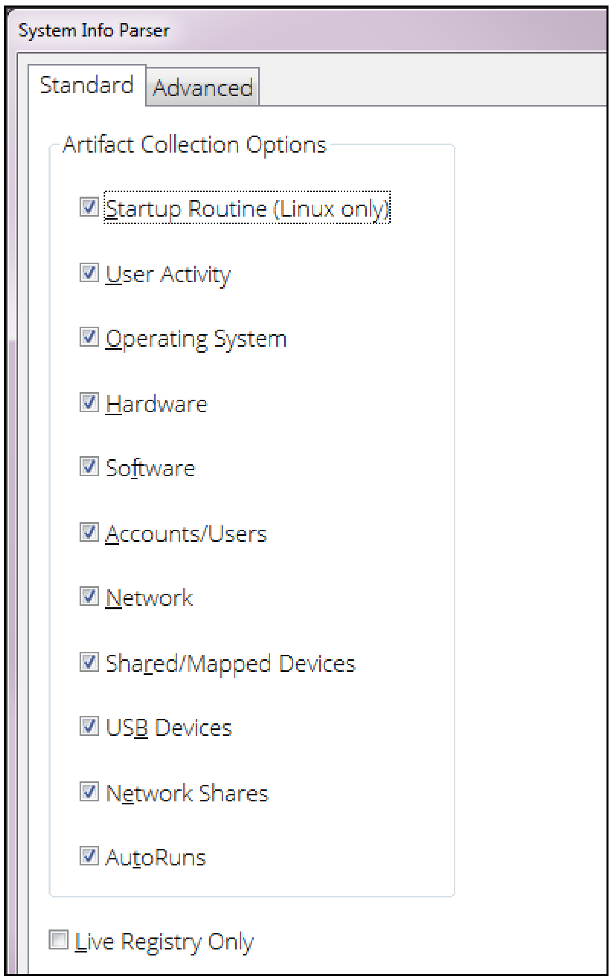
> **Note:** To make a copy of your custom code and modify it while still preserving the original, use the **Save As** option in the dropdown menu.

The EnScript modules included with EnCase are introduced below.

> **Note:** You cannot modify a network tree via an EnScript.

System Info Parser

Use the System Information Parser module to identify hardware, software, and user information from Windows and Linux computers. The module automatically detects the operating system present on the device, then collects the specified artifacts.



Use the **Standard** options tab for both Windows and Linux evidence, with exceptions noted in the user interface. They contain basic information categories for use in reports.

The **Advanced** tab scans for registry information on Windows devices only.

When evidence processing is complete, you can also search **NetShare** and **USB** registry information in the **Artifacts** tab. You can see the UNC path visit history, the history of connected devices, and you can correlate USB devices to their drive letters.

System Info Parser Live Registry Analysis

The System Info Parser includes an option to focus on live registry in memory.

When selected, this option performs a quick sweep against registry entries only resident in memory (versus disk), reducing time taken to analyze live machines.

> **Note:** In the Evidence Processor System Info Parser dialog, the **Live Registry Only** checkbox is cleared by default.

File Carver

The File Carver module allows you to search evidence for file fragments based on a specific set of parameters, such as known file size and file signature. It can also examine unallocated space. It searches for file fragments anywhere on the disk. By default, the File Carver automatically checks file headers for file length information and uses the actual number of bytes carved. You can set specific parameters for carving a file (file size and destination) with the File Carver **Export Settings** dialog. To add an additional file type to carve for, you must add an entry with header information and, optionally, footer information, to the File Types table.

The File Carver is not designed to handle multiple headers and footers. Any file containing more than one header and footer may produce inconsistent results.

Running the File Carver in Evidence Processor gives you three options: you can select from either the full File Types table, from the optimized File Types table, or from both. You can blue check entries and choose to search selected files. The HTML files that the module carves are adjudicated to be HTML, based on certain keywords appearing in the files.

You can export carved files to disk so they can be loaded with native applications.

> **Note:** When there is no file length information in the header, the footer or the default length is used. The value of 4096 bytes is the default carve size when no footer is provided and no default length is provided in the File Types table.

Carving Images with File Carver

The File Carver uses GDI libraries to accurately carve images according to their sizes and file types. GDI libraries identify the actual length of the file to be carved, resulting in increased probability of carving high fidelity images.

GDI libraries handle these file types:

- .jpeg
- .ico
- .gif
- .png

File Carver does not separately carve thumbnails embedded within JPEG images. To carve out the thumbnails embedded in JPEG images, you must add a file type to the File Types table that contains the same information in the JPEG Image Standard fields, with two exceptions:

- The header must read "\xFF\xD8\xFF\xDB".
- The Unique Tag field must consist of four characters beginning with the letters "jpg" and must not conflict with an existing unique tag.

FILE CARVING PROCESS

1. Files are first identified by their file signatures, as defined in the File Types table.
2. When the File Carver module finds a header matching one of the supported image types, it attempts to determine an image size from the GDI libraries.
3. If the GDI libraries return a size, a file of that size is carved.
4. If the GDI libraries do not return a size, File Carver carves the file using the standard method.

CARVED FILE NAMING

Carved files are named as follows: "<sn>_<fn>_FO-<fo>_PS-<ps>+<po>.<ext>"

- <sn>: an incrementing serial number
- <fn>: the name of the entry (filename)
- <fo>: file offset where file header was found
- <ps>: physical sector of file offset
- <po>: offset from beginning of physical sector corresponding to file offset
- <ext>: the first file extension associated with the found file header bytes

> **Note:** The serial number (<sn>) ensures that the output filename of each carved file is unique. it is an eight digit zero-filled number beginning with 00000001. Serial numbers are created when files are exported.

The File Carver changes the output name of files carved from E01/Ex01 files so that physical sector and physical offset values are included in the name, in addition to the file offset values already present. This requires no configuration.

Running File Carver

To process evidence with File Carver:

1. Select the **Evidence** tab and click the checkbox next to the evidence you want to process. From the Process Evidence dropdown menu, click **Process**.
2. The Evidence Processor Current processing options screen displays. Select **Modules** > **File Carver**. The File Carver window displays with your selected options.
3. Click **OK**.

A dialog displays briefly indicating the evidence processing has begun. The lower right corner of the window displays a flashing green Processing indicator until evidence processing completes.

Windows Event Log Parser

The Windows Event Log Parser module parses and collects information pertaining to Windows events logged into system logs, including application, system, and security logs. The module parses .evt and .evtx files for Windows Event Logs, and also allows for processing by condition.

Conditions restrict which files to look at and what entries to parse.

- **Entry condition** filters which files EnCase processes, based on their entry properties.
- **EVT condition** restricts individual events on properties parsed from an EVT file (Event ID, Event Type, Source, etc.).
- **EVTX condition** restricts individual events on properties parsed from an EVTX file (Event ID, Process ID, Thread ID, etc.).

To enable a condition, select its checkbox. Click Edit next to the condition type to modify the condition.

Windows Artifact Parser

The Windows Artifact Parser allows you to search for common Windows operating system artifacts of potential forensic value and parse them through a single module. Artifacts of interest include:

- Link files
- Recycle Bin artifacts
- MFT transaction logs

With these artifacts, you can search unallocated, all files, or selected files. Once the artifacts are parsed, you can browse through the results in the **Artifacts** tab. You can also index the artifacts so they are searchable. In addition, you can bookmark the artifacts.

Unix Login

This module parses files with the names "wtmp" and "utmp," but also allows for processing by condition.

Linux Syslog Parser

This module parses the Linux system Log files, which have different names and locations depending on the type of Linux used.

You can process files by signature and use EnScript code to specify either entry or log event conditions.

Macintosh OS X Artifacts Parser

The EnCase Macintosh OS X Artifacts Parser gathers information from Macintosh computers. Artifacts from Macintosh OS X versions 10.6, 10.7, and 10.8 are supported. This module identifies artifacts typically stored in Mac OS X Property Lists (plist) or log files.

Running the Macintosh OS X parser in EnCase Evidence Processor creates a Logical Evidence File (LEF).

MACINTOSH OPERATING SYSTEM ARTIFACTS

- Operating System version
- Operating System installation date
- Operating System updates
  - This parses the log file, creating artifacts for easy access and review.
- Software updates
  - Last successful software update date
  - Last attempt date
  - Last result code
- Removable USB disks
  - Connected USBMSC devices
- Network connections
  - MAC address of wireless network

- Network configuration settings
    - Network adapters
    - Host and computer names
    - Network services
    - Network configuration
    - Wireless networks
    - Internet sharing
    - Firewall settings
- Time zone settings
- Last user and auto-login settings
- Deleted user accounts
- Trash
    - "Put Back" .DS_store analysis
    - Deletion time
- iOS device information

MACINTOSH USER ARTIFACTS

- Recent items
- Folders visited
- Folders visited with finder
- Folders visited with the common file/folder navigation dialog
- Attached media and connected servers
- Favorite servers

Startup applications

- Saved searches
- Printing activity

Artifacts parsed are inserted into a SQLite database. Case Analyzer reports contain data for the artifacts generated by the Macintosh OS X Artifact Parser module.

CASE ANALYZER MACINTOSH REPORTS

After running the Macintosh OS X Artifacts Evidence Parser, data collected is available in Case Analyzer Macintosh reports.

The following reports are created, based on the information collected by the Macintosh OS X Artifacts Parser:

- Accounts and Users
  - OS X Deleted Users Report
  - OS X Users Report
- Drives Removable + Local
  - OS X Attached Media Report
  - OS X IOS Devices Report
  - OS X USB Devices Report
- Drives Shared + Network
  - OS X Network File Activity Report
- File Activity > Documents
  - OS X Recent Files Report
- Multimedia
  - OS X Recent Files Report
  - OS X Saved Searches Report
- Logins and Boots
  - OS X User Session Event Report
- Network
  - OS X Network Interfaces Report
- Operating System
  - OS X Install Log Report
  - OS X System Overview Report
- Software Usage and Autorun
  - OS X Recently Used Applications Report

Double Files

Double files are artifacts created by OS X.

The HFS+ file system supports extended attributes, such as Finder attributes and the location of a file within the Finder coordinates X and Y. They are in the **Attributes** tab in EnCase.

When OS X writes to a file system that does not support extended attributes (for example, FAT or exFAT), a double file is created in the same location as the actual file that is written to store the extended attributes the HFS+ needs. So if the file is ever copied back to an HFS+ formatted drive, the attributes are included along with the file itself.

Double files have the prefix ._

Extended attributes in HFS+ are stored in double files.

X:DateAdded

X:DateAdded indicates the time a file was added to the parent folder. For example, X:DateAdded to the Trash folder represents the time the file was deleted.

Keychain Parsing

OS X keychains provide a secure way to store passwords, certificates, and notes. Whenever OS X asks if you want to remember a password, it is stored in a keychain.

The user keychain is typically located in \Users\<user>\Library\Keychains.

When you are investigating a Mac:

1. Locate the keychain.
2. Click **Entries** > **View File Structure**.
3. The View File Structure dialog displays. Enter a password and click **OK**.

    Note: If you do not know the password, there are tools (such as Passware Forensic) that can perform keychain attacks.

Once the keychain is parsed, you can view the contents as artifacts.

If a keychain's password is known, secrets in the keychain are parsed and stored in Secure Storage in EnCase.

For details on keychain parsing, refer to these posts in the Guidance Software blog *Digital Forensics Today*:

- http://encase-forensic-blog.guidancesoftware.com/2014/04/encase-70904-extracting-passwords-from.html
- http://encase-forensic-blog.guidancesoftware.com/2013/07/examining-mac-os-x-user-system-keychains.html

STREAMLINED DMG DECRYPTION

If credentials are parsed and stored in Secure Storage, EnCase automatically decrypts and mounts the .dmg file.

1. View File Structure on a .dmg file: in the Entries dropdown menu, click View File Structure and select the .dmg file.
2. The View File Structure dialog displays. Click **OK**. You do not need to enter a password.
3. The .dmg file mounts and its contents are decrypted.

Result Set Processing

You can process a result set from a case for specific information you want to review, instead of running Evidence Processor for an entire device.

Processing a Result Set

1. Open the Processor Options dialog. Depending on the context, there are several ways to do this. For example, in the **Evidence** tab, click **Process Evidence** > **Process**.
2. Click **Result Set**. The Process Result Set dialog displays.
3. Select the result set you want to process, then click **OK**. The EnCase Processor Options dialog displays a table with information about the result set to be queued:
   - Name
   - Evidence Size
   - Item Logical Size
   - Item Count

   This information helps you identify the size and scale of the evidence to be processed. A result set can contain items from multiple evidence files, all of which will be processed.
4. Click **OK**. EnCase begins processing the evidence.

Note: Processing modules (System Info Parser, File Carver, Windows Artifact Parser, etc.), along with Recover Folders, do not respect result sets and therefore run against the entire device as they normally do.

Note: Because result sets can include items from multiple devices in various processing states, locks do not display in processing options when selecting result set processing. However, items that would normally be locked because they were previously run on a device will still run, even if they do not have the lock item present. In other words, once a lockable Evidence Processor option is run on a device, all processing jobs that follow on that device will run the option, even if it is not selected. The screenshot in Step 3 above explains that these previously processed items are marked with asterisks, and those items will be reprocessed.

Note: Also, since locks do not display, some modules that are not supported in certain instances will not run, even if they are selected. For example, indexing will not run on items that come from a remote node, and Snapshot will not run on an evidence file or a local drive.

Launching Processor Options from the Results Tab

You can open the EnCase Processor Options dialog from the **Results** tab. This saves time by giving you the option to process only the evidence you want to examine.

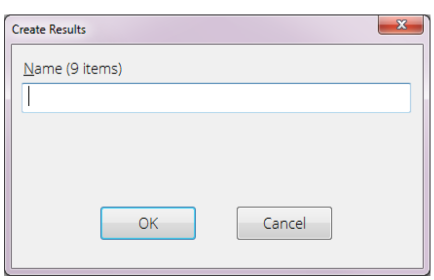
1. In the **Results** tab, select the result set you want to process.
2. Right click, then click **Process** in the dropdown menu.
3. The EnCase Processor Options dialog displays.

Creating Result Sets in Entries and Artifacts Views

You can create a result set similar to the way you create a Logical Evidence File. The menu is accessed from Entries or Artifacts view, as described below.

Creating a Result Set in Entries View

1. In the Tree and/or Table pane, blue check the items you want to include in the result set.
2. Right click, and in the dropdown menu click **Entries** > **Create Results**.
3. The Create Results dialog displays, showing the number of items selected that are under the highlighted folder.



To include all blue checked items in a device, highlight the device root first before selecting the **Create Results** option.

4. Enter a name for the result set, then click **OK**.
5. EnCase creates the result set, and it displays in the **Results** tab.

Creating a Result Set in Artifacts View

In Artifacts view, you can create result sets from mounted items that are not metadata only.

Some examples of data types that allow creation of result sets include:

- Email archives
- Compound files (for example, .zip files)
- Internet artifacts

Examples of data types that do not allow creation of results (because they are metadata only) include:

- Snapshot data
- System Info Parser results
- Windows Artifact Parser results
- Windows Event Log Parser results

To create a result set in Artifacts view:

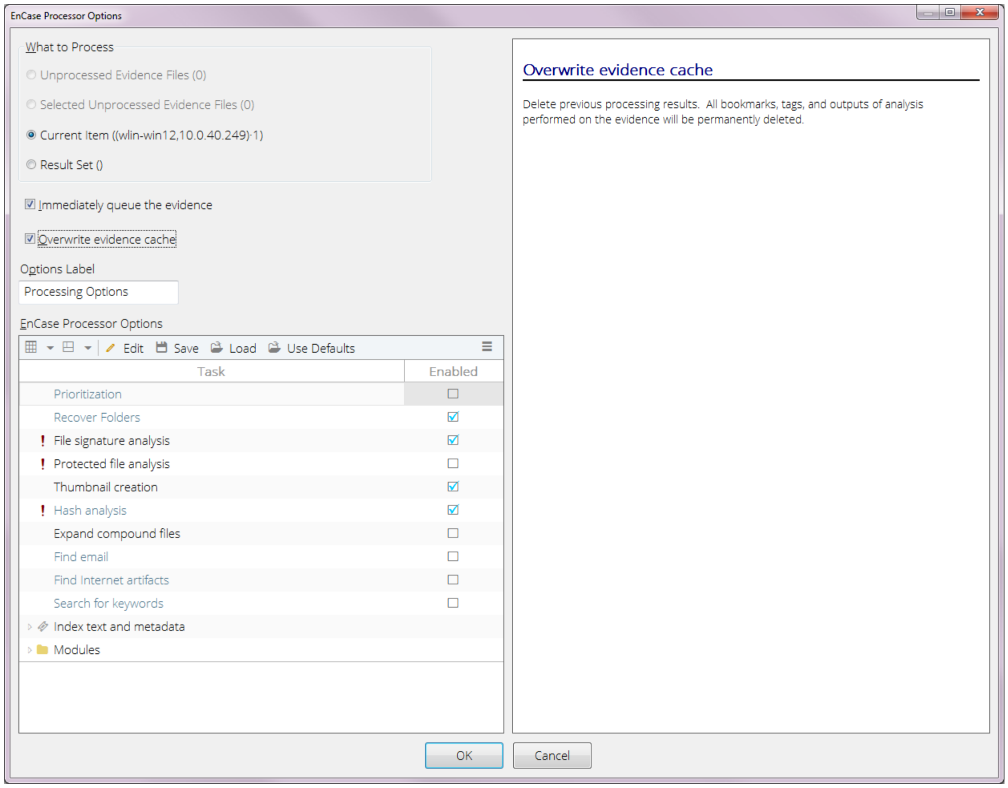
1. In the Tree and/or Table pane, blue check the items you want to include in the result set.
2. Right click, and in the dropdown menu click **Artifacts** (or **Entries**, depending on the context) > **Create Results**.
3. The Create Results dialog displays, showing the number of items selected.
4. Enter a name for the result set, then click **OK**.
5. EnCase creates the result set, which displays in the **Results** tab.

Overwriting the Evidence Cache

The Overwrite Evidence Cache option enables you to delete previous processing results for the selected item and restart processing.

> **Note:** Use this option with caution, as it will remove all processing results for the devices selected.

1. Click the **Overwrite Evidence Cache** checkbox. An information message displays in the right pane.



Note: This option is enabled only when you select **Current Item** and the evidence is already processed.

2. Click **OK**. A warning message displays, asking if you want to continue and delete previously processed output.
3. To continue, click **Yes**. EnCase will delete all caches related to the specified evidence file.

Note: When you use the **Overwrite Evidence Cache** option, items in the result sets and bookmarks belonging to the device will no longer resolve to the original item GUIDs and will become invalid. You can delete the existing result sets and bookmarks or maintain them as a reference for manual recreation.

EnScript Application UI

There are links on the Home and Case pages for EnScripts. There is also a package details page.

Home Page

On the Home page, there is an **EnScripts** link in the View section.

Click the link to go to the EnScripts page. This page displays the most recently used scripts.

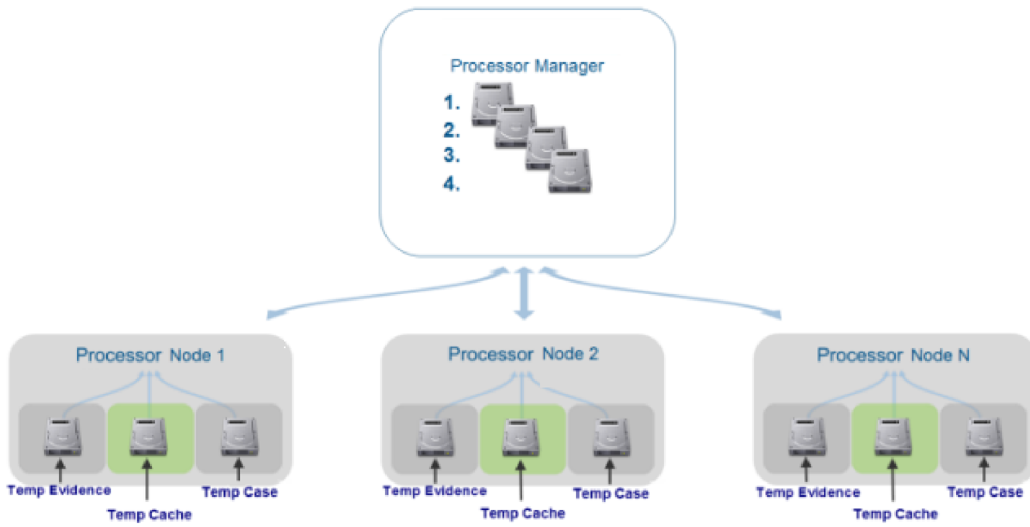
Case Page

On the Case page, there is an EnScripts link in the Browse section.

Click the link to go to the EnScripts page.

Processor Manager

The Processor Manager allows for distribution and control of evidence processing for one or more EnCase Examiners or EnCase Processors.



With Processor Manager, you can simplify evidence processing and acquisition by:

- Queuing evidence in the jobs list to be processed. A job is defined as evidence combined with processor options.
- Prioritizing execution of evidence to be processed.
- Distributing the processing workload across multiple processing nodes. Any available node picks up the next job in the queue, so the evidence is processed as quickly as possible.

You can process evidence locally or over a network.

For a table showing terms and definitions for the Processor Manager, see Terms and Definitions on page 173.

Processor Node Installation

For installation instructions, see Install and Configure Evidence Processor Nodes on page 51 in the Installing and Configuring EnCase chapter of this book.

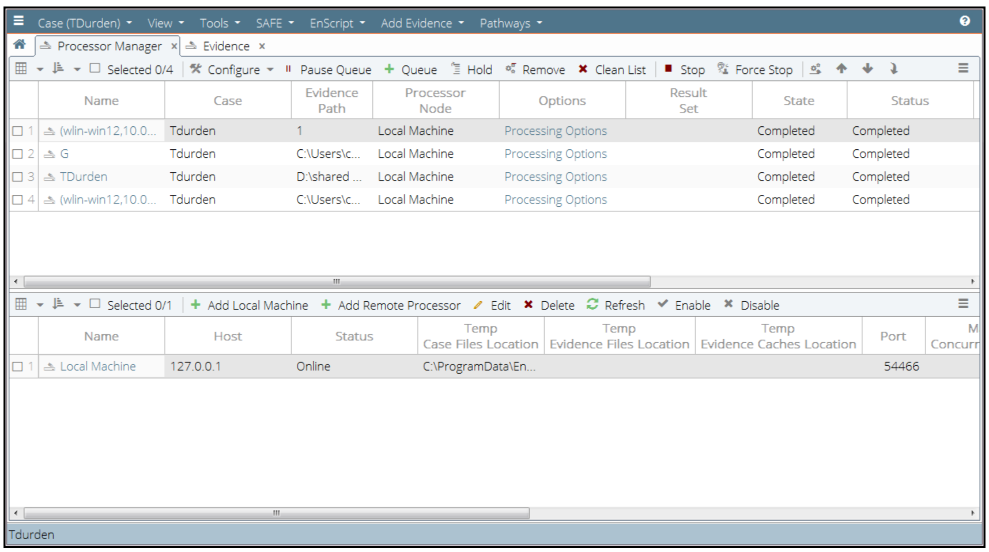
Opening the Processor Manager

To access the Processor Manager:

1. On the EnCase Examiner home page, click **Processor Manager**.

   Note: If both EnCase Examiner and the EnCase Processor Node are installed on the same machine, be sure to open EnCase from the EnCase Examiner shortcut. Using the shortcut that comes with Processor Node generates errors.

2. The **Processor Manager** tab displays.



Adding Processor Nodes to the Processor Manager

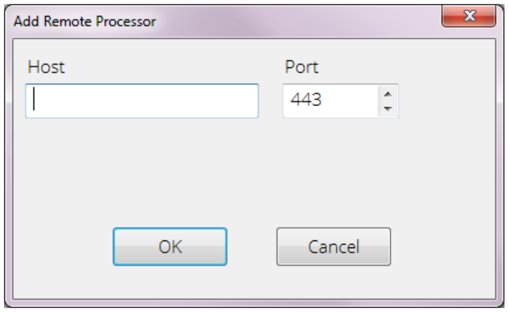
After installation of the Processor Node, you must configure the processor nodes you want to use.

Adding a Local Machine to the Processor Node List

1. In the lower pane of the **Processor Manager** tab, click **Add Local Machine**.
2. The Add Local Machine dialog displays.
3. EnCase adds your local machine to the processor node list and closes the dialog.

Adding a Remote Processor to the Processor Node List

1. In the lower pane of the **Processor Manager** tab, click **Add Remote Processor**.
2. The Add Remote Processor dialog displays.



3. In the Host box, enter the machine name or IP address.
4. In the Port box, enter the port number or use the up or down arrows to scroll to the port number you want to use. The default port is 443.

> **Note:** If you enter a name and port for an existing node, an information message displays telling you the node is already in the list. If the node you are adding has the same name as a node already in your list, the new node is renamed by adding "New" to give it a unique name.

5. Click **OK**. The node is added to the list.

> **Note:** If you get an error after clicking **OK**, the EnServer service on the Processor Node may be stopped. Start the EnServer service and try again.

Checking Evidence Processor Settings and Jobs

Click the name of a node to see a web page displaying the processor node's configuration settings and the contents of its job list.

You can also use a web browser from any machine that can connect to your processor node and manually enter the processor node's URL.

> **Note:** A warning may display in the web browser saying the site's security certificate is not trusted. This is expected behavior, and you can click through the message to proceed.

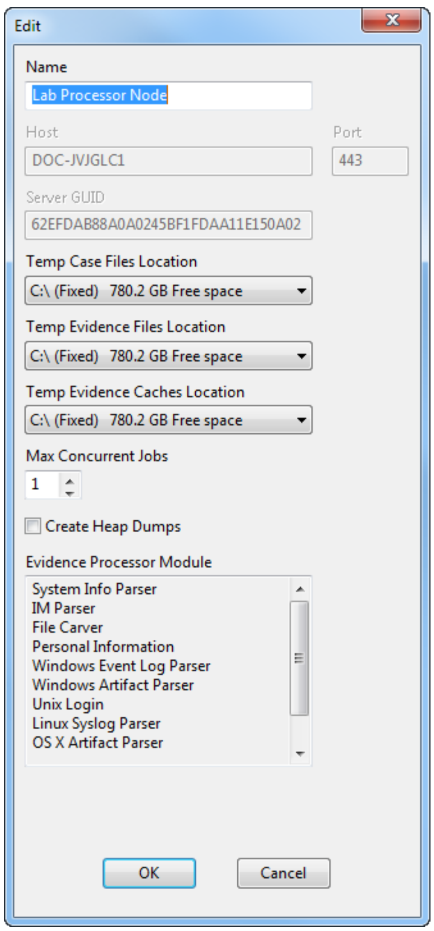
Configuring Processor Nodes

You can edit existing remote processor nodes to change or specify:

- The name of the processor node. The name cannot match any processor node already in the list.
- Storage configuration (temp case files location, temp evidence files location, temp evidence caches location).
- The number of maximum concurrent jobs.
- Whether to create heap dumps.

Note: You cannot edit a local machine node.

1. In the lower pane of the **Processor Manager** tab, select the node you want to edit, then click **Edit**.
2. The Edit dialog displays. Enter your desired changes.



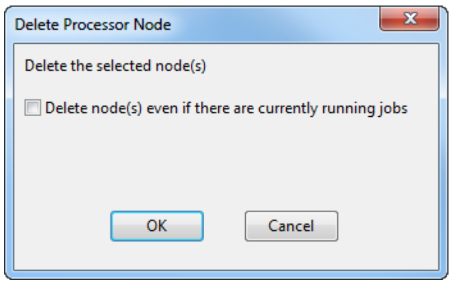
Note: A heap dump is a file containing a snapshot of the memory of a Windows process that terminated abnormally. If you select the **Create Heap Dumps** checkbox, when a crash occurs during processing, a heap dump is created and saved on the processing node. You can then send the heap dump to Guidance Software for analysis.

3. When you are finished, click **OK**.

Deleting Processor Nodes

To delete a processor node:

1. In the lower pane of the **Processor Manager** tab, select the node you want to delete. If you want to delete more than one node, click the checkboxes for those nodes.
2. The Delete Processor Node dialog displays.



3. If a node or nodes are running jobs and you still want to delete them, click the **Delete node(s) even if there are currently running jobs** checkbox.
4. Click **OK**.

Note that:

- You cannot delete the Local Machine processor node if a job is currently running on it.
- Jobs running on a remote processor node that is deleted and removed from the processor list continue to run on the node. However, the job's status in Processor Manager will change to "Processor Node is Unknown" and the processing state is set to "Pending." If you add that processor node back into the list, the job's state and status are updated to show the true status of the job running on that node: "Running," "Error," or "Completed".

Process Evidence Menu

The Process Evidence menu on the **Evidence** tab contains three options:

- **Process**: Use this to combine evidence with processor options to create a job.
- **Acquire**: Use this to acquire evidence without processing it.
- **Acquire and Process**: Use this to acquire evidence first and then process it.

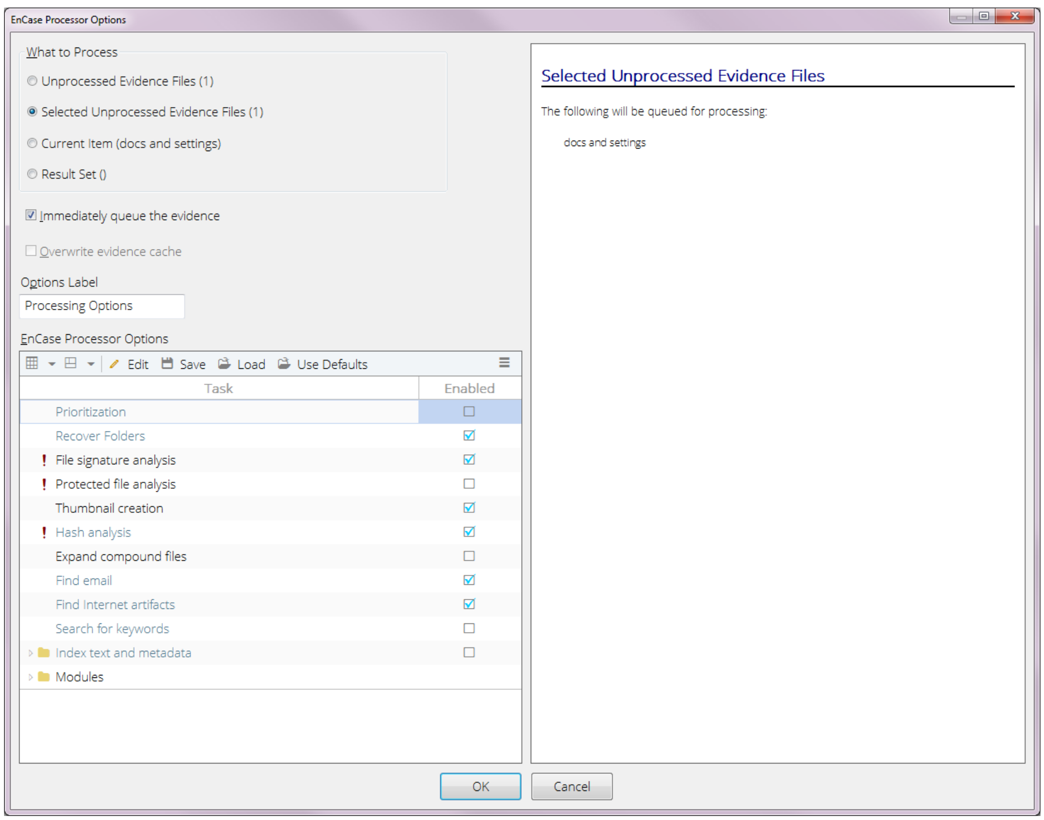
Queuing Evidence for Processing

To queue evidence for processing:

1. Open the case containing the evidence you want to process.
2. On the **Evidence** tab, select the checkboxes for the unprocessed evidence you want to process, then click **Process Evidence** > **Process**.

   Note: If you select no checkboxes, all unprocessed evidence in the case is set to be added to the queue.

3. In the dropdown menu, click **Process**.
4. The EnCase Processor Options dialog displays.



5. The evidence files to be queued for processing, and the information that displays in the right pane, depend on which **What to Process** radio button you select:
   - **Unprocessed Evidence Files**: Includes all unprocessed evidence files in the case.
   - **Selected Unprocessed Evidence Files**: Includes only the evidence files you selected on the **Evidence** tab.
   - **Current Item**: The item currently highlighted on the **Evidence** tab.

- ◦ **Result Set**: Select this option to process a result set. For more information, see Result Set Processing on page 162.

6. Click the **Immediately queue the evidence** checkbox if you want to put the selected items in a job list to be executed by the next available node now. If you do not check the box, the items are put in the Processor Manager in an On Hold status.
7. The **Overwrite evidence cache** option, if available, enables you to delete previous processing results for the selected item and restart processing.
8. In the Options Label box, enter a label or accept the default, Processor Default Options.
9. The first option, **Make local copies**, copies the evidence to the assigned remote Processor Node. The Processor Node displays:
   - ◦ Temp evidence cache location.
   - ◦ Temp evidence files location.
   - ◦ Temp case files location.

   Note: If Local Machine is the only processor node in the node list, the **Make local copies** option is not available. This option is only available if there are remote processor nodes in the node list.

   Advantages to using **Make local copies** include:

- If there are network interruptions, there is no cache corruption because the cache is created locally on the node before it is uploaded to the shared drive.
- If the network is slow, it does not impact processing because all processing is done locally on the node before it is uploaded to the shared drive.

   Once the processing completes, the cache is copied to the shared network drive. Then the evidence file and cache are deleted from the remote node.

10. When you finish selecting what evidence to process and the processing options you want, click **OK**.
11. A dialog displays showing that the evidence to be processed is loading.

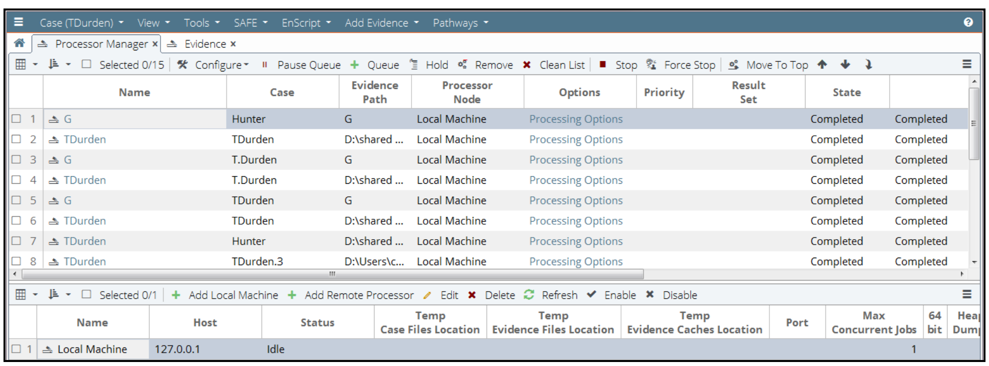
   For detailed information on other evidence processing options, see the following topics in this book:

   - ◦ Evidence Processor Prioritization on page 133. If you choose the Prioritization option, EnCase puts two jobs into the Processor Manager job list. The first job is for the prioritized items in the evidence. The second job is for all the remaining (that is, not prioritized) items in the evidence that were not processed by the first job.
   - ◦ Recovering Folders on page 135.
   - ◦ Analyzing File Signatures on page 138.
   - ◦ Analyzing Protected Files on page 135.

- Creating Thumbnails on page 153.
- Analyzing Hashes on page 136.
- Expanding Compound Files on page 138.
- Finding Email on page 139.
- Finding Internet Artifacts on page 139.
- Searching With Keywords on page 143.
- Creating an Index on page 148.
- System Info Parser on page 154.
- File Carver on page 155.
- Windows Event Log Parser on page 157.
- Windows Artifact Parser on page 157.
- Unix Login on page 158.
- Linux Syslog Parser on page 158.
- Macintosh OS X Artifacts Parser on page 158.

Processor Manager Tab

1. On the EnCase Forensic home page, click **Processor Manager**, or from the menu bar click **View** > **Processor Manager**.
2. The **Processor Manager** tab displays.



Terms and Definitions

This table shows terms and definitions for the Processor Manager.

Term	Definition
Job	Evidence combined with processor options.
Job List	All jobs in the Processor Manager. The job list displays in the Name column of the top pane of the Processor Manager.

Term	Definition
Queue	Jobs in the list to be processed.
Hold	Evidence in the list not to be processed.
Pause Queue	Stops distributing jobs to processor nodes (jobs that are executing will continue).
Priority	Order of execution relative to unprocessed jobs.
Processor Node	Name of a processor node (set during installation).
Options	A collection of processing configurations assigned to an individual job.

Job Actions Menu

The Job Actions menu includes eight options.

TO REMOVE JOBS FROM THE JOB LIST

1. Select the checkboxes for the jobs you want to remove from the job list entirely.
2. Click **Job Actions** > **Remove**. A warning message displays asking if you want to remove the selected jobs from the list. Click **Yes**.

TO MOVE A JOB TO THE TOP OF THE JOB LIST

Note: A job must be in Queued state to move it to the top.

1. Select the checkboxes for the jobs you want to move to the top.
2. Click **Job Actions** > **Move to Top**. The selected items are moved to the top of the list of queued jobs.

TO INCREASE THE PRIORITY OF A JOB

Note: A job must be in Queued state to increase its priority.

1. Select the checkboxes for the jobs you want to increase in priority.
2. Click **Job Actions** > **Increase Priority**. The selected jobs move up in the list in the Priority column and have a higher priority.

TO DECREASE THE PRIORITY OF A JOB

Note: A job must be in Queued state to decrease its priority.

1. Select the checkboxes for the jobs you want to decrease in priority.
2. Click **Job Actions** > **Decrease Priority**. The selected jobs move down in the list in the Priority column and have lower priority.

TO MOVE A JOB TO THE BOTTOM OF THE JOB LIST

> **Note:** A job must be in Queued state to move it to the bottom.

1. Select the checkboxes for the jobs you want to move to the bottom.
2. Click **Job Actions** > **Move to Bottom**. The selected jobs are moved to the bottom of the list of queued jobs.

RIGHT CLICK JOB ACTIONS

If you select a job and right click, you can:

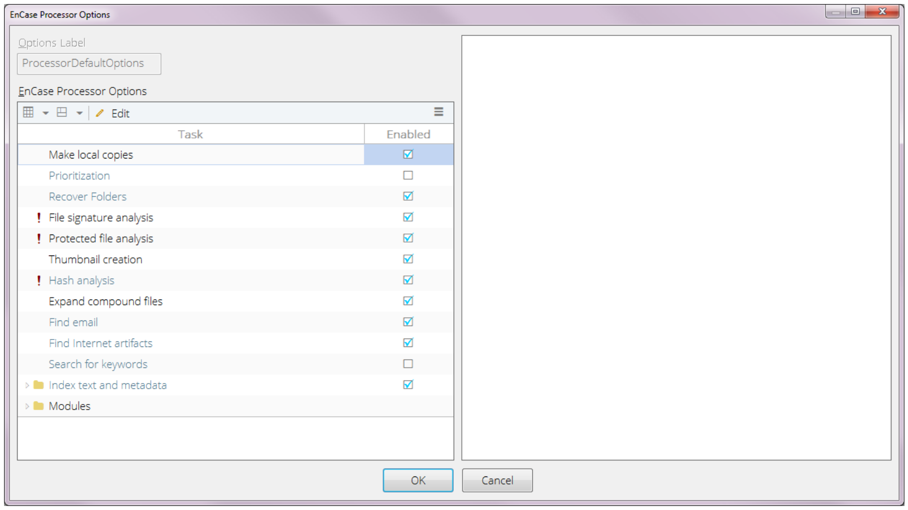
- Queue
- Remove
- Hold
- Stop
- Change job priority
- Copy (Available on the right click menu only: This option copies the text in the currently highlighted field in the currently highlighted row.)

> **Note:** These right click actions only operate on the currently highlighted job; however, actions in the Job Actions menu of the **Processor Manager** tab work for all blue checked items.

Editing Default Options

Edit Default Options enables you to make changes to the default processing options for selected jobs in the list.

1. Select the checkboxes for the jobs whose processing options you want to edit.
2. Click **Configure** > **Edit Default Options**. The EnCase Processor Options dialog displays with the default processing options selected.



3. Make the changes you want, then click **OK**.
4. Options are changed for the selected items.

Set Manager Name

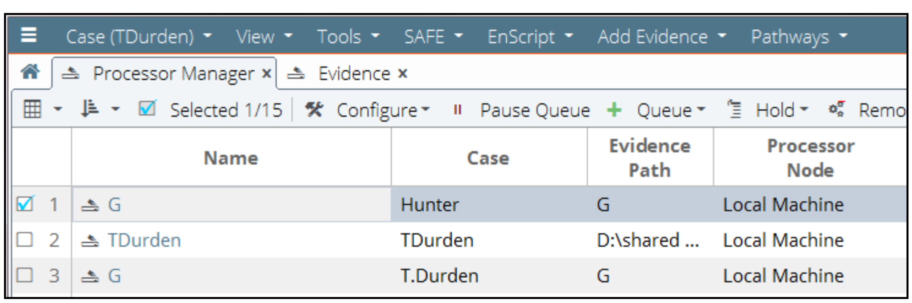
This option sets a name for your specific processor manager. It is only relevant for labs where there are multiple processor managers sharing a group of processor nodes. By default, your manager name is the name of your computer.

To set the manager name:

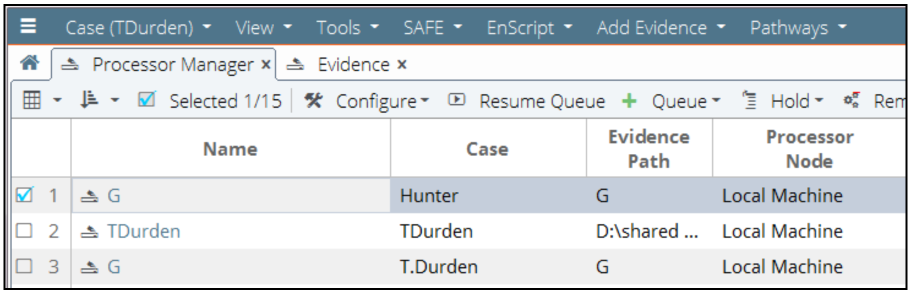
1. Click **Configure** > **Set Manager Name**. The Manager Settings dialog displays.
2. Enter the manager name you want to use, then click **OK**.

Pause Queue

The **Pause Queue** button is a toggle. Use the Pause Queue button to pause submission of new jobs to the Evidence Processor.



1. Click **Pause Queue** once to pause submission of new jobs. Current jobs continue to execute. The menu name changes to **Resume Queue**.



2. Click **Resume Queue** to resume submitting jobs to the Evidence Processor.

Clean List

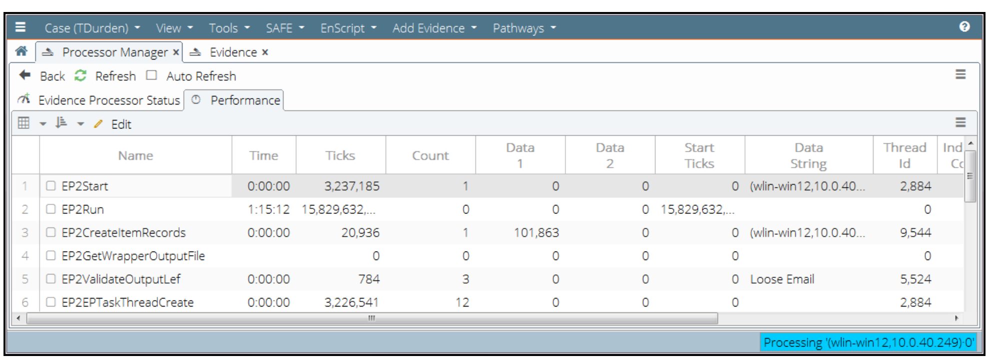
The Processor Manager **Clean List** menu button removes all processed and failed jobs from the job list. Processing, Queued, and On Hold jobs remain in the job list.

1. Click **Clean List**. A dialog displays asking you to confirm before removing all processed and failed jobs from the job list.
2. Click **Yes**.

Performance Monitoring

Monitor evidence processor performance in the Processor Manager tab. Click on the name of a job to display the following two tabs:

- The **Evidence Processor Status** tab displays, providing information on the job currently running. It shows what is executing within a given job from the node that is processing the job, as well as basic memory information.
- The **Performance** tab displays the current state of the performance counters for the selected job.



Click **Back** to return to the job list, click **Refresh** to instantly refresh the performance statistics, or click the **Auto Refresh** checkbox to enable periodic updates of performance statistics.

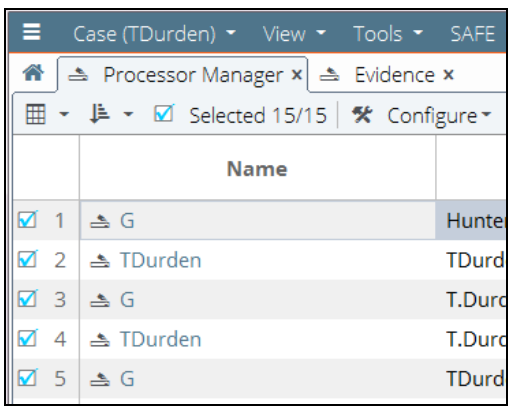
Processor Manager Toolbar

The Processor Manager toolbar provides the ability to launch various actions and to control the way information is displayed (for example, sorting the jobs list or showing or hiding columns). The functionality of each toolbar item is explained in detail below.

Selecting/Clearing All Jobs

To select all items in the job list at once:

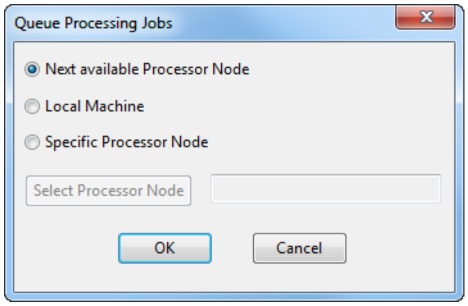
1. Click the **Selected #/#** checkbox above the Name column.



2. Click the checkbox again to clear all selections.

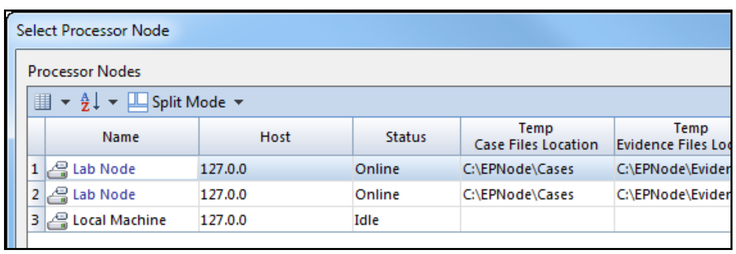
Queue

1. Select the job you want to queue for processing. If you want to queue more than one job, click the checkboxes for those jobs.
2. Click **Queue**. If you clicked more than one checkbox, you have the option to queue only the currently selected job or all the selected jobs.
3. From the dropdown menu, click **Current Item** or **All Selected Items**. The Queue Processing Jobs dialog displays.



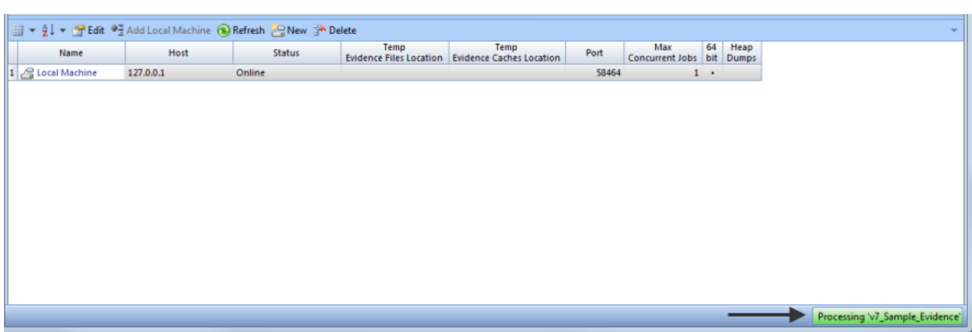
Note: This dialog does not display if Local Machine is the only node in the node list.

- Select **Next Available Processor Node** to send the job to the most currently available Processor Node. This is the default.
- Select **Local Machine** to process the job locally instead of sending it to a Processor Node.
- Select **Specific Processor Node** if you want choose a specific Processor Node to use to process the job. The **Select Processor Node** button is then enabled. Click the button to open the Select Processor Node dialog.



- Select the Processor Node (in online status) you want to use, then click **OK**. Back in the Queue Processing Jobs dialog, click **OK**.

4. An indicator in the bottom right corner shows which evidence is currently being processed. You can double click this indicator at any time to go to the **Processor Manager** tab.



You can see processing details in the Event Viewer of the machine running the Processor Node. You will see:

- "Job [GUID] Evidence Processing successfully registered."
- A log showing the job was created.
- A log placing a marker file.

You will see logs each time an event begins (for example, processing starts and threads created).

Hold

To place a job on hold:

> **Note:** A job must be in Queued state to place it on hold.

1. Select the job you want to place on hold. If you want to place a hold on more than one job, click the checkboxes for those jobs.
2. Click **Hold**. If you clicked more than one checkbox, you have the option to place only the selected job on hold or all the selected jobs.
3. The Hold Job(s) dialog displays, asking if you are sure you want to place the job(s) on hold. To continue, click **Yes**.
4. The state of the selected jobs changes to On Hold.

Stop

To stop a job:

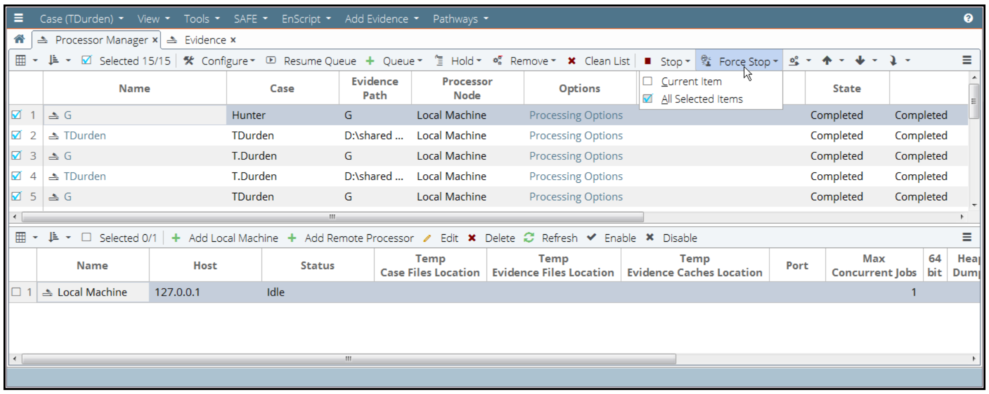
1. Select the job in a running state that you want to stop processing. If you want to stop more than one job, click the checkboxes for those jobs.
2. Click **Stop**. If you clicked more than one checkbox, you have the option to stop only the selected job or all the selected jobs.
3. The Stop Job(s) dialog displays, asking you to confirm stopping the selected job(s). Click **Yes** to continue.
4. The state of the selected jobs changes to Incomplete.

Force Stop

You can use Force Stop if a job fails to stop successfully. There is no specific amount of time you should wait before deciding to use Force Stop. It depends on the evidence you are processing and what processing has already occurred at the time you tried to stop the job. Some evidence can take minutes to stop processing; however, it is safe to assume something is wrong if the job does not stop after tens of minutes.

To force stop a job:

1. Select the job you want to force stop. If you want to force stop more than one job, click the checkboxes for those jobs.
2. Click **Force Stop**. If you clicked more than one checkbox, you have the option to force stop only the selected job or all the selected jobs.



3. The Force Stop dialog displays, asking you to confirm termination of the job. Click **Yes** to continue.
4. The state of the job changes to Incomplete.

Running Multiple Instances of EnCase from the Same Machine

Investigators can queue and manage jobs using multiple instances of EnCase Processor Manager on the same machine. When running multiple instances, however, you cannot see the position of a specific job in the queue.

Processor Manager Error and Information Messages

The table below lists the most common Processor Manager error and information messages with an explanation of why you would see them.

Message	Explanation
Waiting for job state from Processor Node.	You may see this job status briefly when you start EnCase and quickly switch to the **Processor Manager** tab. The status message is for jobs in the job list that EnCase last identified as running on a remote processor node. The job status is quickly replaced with either the actual job status or "Waiting for Processor Node to come Online" if the node is offline.
[processor node name] is not in the Processor Node list.	Jobs display this status when the processor node they are queued to or running on is deleted from the node list. The status goes away if the node is added back into the list.
The chosen Processor Node cannot access the evidence file.	Jobs display this status when they are queued to a specific processor node, but the processor node cannot access the job's evidence file over the network.
The chosen Processor Node cannot access the primary evidence cache folder.	Jobs display this status when they are queued to a specific processor node, but the processor node cannot access the job's evidence cache over the network.
The chosen Processor Node does not have the module [module name].	Jobs display this status when they are queued to a specific processor node, but the processor node does not have the indicated third party EnScript module required by the job.

Message	Explanation
No Processor Node can access both the evidence file and evidence cache.	Jobs queued to the next available processor node display this status when none of the processor nodes can access the job's evidence file and evidence cache over the network. Jobs in this status remain in the Queued state and will run if the network access issue is fixed.
No Processor Node has the module [module name].	Jobs queued to the next available processor node display this status when no processor node has the indicated third party EnScript module required by the job.
Corresponding job [parent job name] failed to complete.	A child job displays this status if its parent job fails to complete successfully. The child job is placed into the error state (or incomplete state if the parent job was stopped). Examples of paired jobs are: • Stage 1 job (parent) and corresponding Stage 2 job (child) • Acquire job (parent) and its corresponding processing job (child), if the **Acquire and Process** option was used.
Not all evidence was queued. See Job Status for more information.	This message displays after attempting to queue jobs if not all of the jobs were successfully queued. You can go to the **Processor Manager** tab to see which jobs failed to queue and why.

Message	Explanation
Job [child job name] cannot be queued because corresponding job [parent job name] is not Queued, Running, or Processed.	A child job displays this status if you try to queue the job, but its parent job is not currently queued, running, or processed at the time you try to queue the child job. Examples of paired jobs are: • Stage 1 job (parent) and corresponding Stage 2 job (child) • Acquire job (parent) and its corresponding processing job (child), if the **Acquire and Process** option was used.
Stage 2 jobs must be queued to the same Processor Node as their Stage 1 jobs.	A Stage 2 job displays this status if you try to queue it to a different processor node than the one to which its parent job was queued.
The evidence is already queued for processing.	A job displays this status when you try to queue it, but there is another (non-parent) job for the same evidence that is already queued.
The evidence is already being processed.	A job displays this status when you try to queue it, but there is another (non-parent) job for the same evidence that is already running.
Running jobs must be stopped before being removed from list.	This message displays if you blue check a number of jobs in the job list, then click the **Remove** menu option, and some of the blue-checked jobs are currently running. The running jobs are left alone. The other jobs are removed.

Message	Explanation
Priority of [child job name] job cannot be increased above that of corresponding job [parent job name].	This message displays if you attempt to increase a child job's priority above that of its corresponding parent job.
Priority of [parent job name] job cannot be decreased below that of corresponding job [child job name].	This message displays if you attempt to decrease a parent job's priority below that of its corresponding child job.
You must wait for the current job to complete before you can remove Local Machine from the list.	This message displays if you try to delete the Local Machine from the processor node list while the Local Machine is processing a job.
You must stop all local processing jobs before closing EnCase.	This message displays if you try to close EnCase while jobs are running on the Local Machine or running internally.

Message	Explanation
Cannot edit the options of a Stage 2 job. Edit the options of the corresponding Stage 1 job instead.	This message displays if you try to edit the processing options of a Stage 2 job present in the job list.
There is already a Processor Node with the name [processor node name].	You see this message if you try to rename a node to a name that matches a node already in the processor node list.
The specified Processor Node is already in the list.	This message displays if you try to add a processor node already in the processor node list.
Processor Node [processor node name] is not compatible with this version of EnCase.	This message displays if you try to add a processor node that is either too new or too old compared to the version of EnCase you are using. This message also displays the version number of the processor node and the version number of your EnCase and indicates which one needs to be updated.
You must have at least one Processor Node.	This message displays if you try to delete the last remaining processor node from the processor node list.

Message	Explanation
All Processor Nodes are offline.	Jobs queued to the next available processor node display this status if all processor nodes go (or are) offline. The status goes away when at least one node comes online.
Acquisition was stopped.	Acquisition jobs display this status if they are stopped before acquisition can complete.
Waiting for case to be opened.	Acquisition jobs in the Queued state display this status if the case the job is associated with is not open in EnCase. Unlike processing jobs, an acquisition job can only run when its case is open.
Waiting for Processor Node to come Online.	A job queued to a specific processor node displays this status when that node is offline. The status goes away when the node comes online. Jobs that were running on that node also display this message while the node is offline.
Evidence must be queued to Local Machine.	This message displays if you try to queue a job to a remote processor node but the job's evidence must be processed locally. Currently, only evidence files can be processed by remote processor nodes. Previews must be processed by the Local Machine.
Local Machine is required but is not configured for processing.	A job displays this status if you try to queue the job and it requires the Local Machine (that is, because job's evidence is a preview), but the Local Machine is not in the processor node list.
Evidence is already queued for acquisition.	An acquisition job displays this status if you try to queue the job but there is another acquisition job for the same device or evidence file already in the queue.
You must select a Processor Node that is Online.	This message displays if you try to queue a job to a processor node that is offline.

Message	Explanation
No valid evidence images to process.	This message displays after the Processor Options dialog closes if none of the evidence you selected for processing can be opened.
No currently available Processor Node can run this job.	Jobs queued to the next available processor node display this status when none of the processor nodes available can run the job. A node is not available if it is currently processing a job. If all nodes become available and yet none of them can process the job, then the job status changes to either "No Processor Node can access both the evidence file and evidence cache" or "No Processor Node has the module [module name]", depending on the reason why the nodes cannot process the job. If a node that can run the job becomes available, it runs the job.
Job not present on Processor Node [processor node name].	A job displays this status if it started running on a processor node and then some time later the node loses knowledge of the job. This can happen if the node is stopped (or crashed) and then restarted.
This EnCase is not the active Evidence Processor Manager.	This message displays if you start a second instance of EnCase from the same installation and then try to process evidence with that EnCase. Only one EnCase from a given install can act as Evidence Processor Manager. If EnCase is installed multiple times into different install folders, then each of them can run as an Evidence Processor Manager.

Message	Explanation
Local Machine cannot be edited.	This message displays if you try to edit the processor node settings of the Local Machine node. In general, these settings cannot be changed. However, you can enable the **Heap Dump** option for the Local Machine in EnCase in the **Tools** > **Options** dialog (on the **Debug** tab). The next time the Local Machine is started, it will run with heap dumps enabled. To disable heap dumps for the Local Machine, first disable it for EnCase, then restart EnCase.
Evidence file path must use UNC or mapped drive.	A job displays this status if it was submitted to a remote processing node for processing but the evidence file path did not use UNC format or a mapped drive letter. Remote processing nodes can only process evidence files residing on shared drives.
Evidence cache path must use UNC or mapped drive.	A job displays this status if it was submitted to a remote processing node for processing but the evidence cache path did not use UNC format or a mapped drive letter. Remote processing nodes can only process evidence files if their evidence cache folders reside on shared drives.
Processor Node cannot write to evidence cache folder.	A job displays this status if it was submitted to a remote processing node for processing but the processing node does not have write access to the case's network-shared evidence cache folder.
The UNC path or mapped drive specified in the case does not resolve to the same location on the Processor Node.	A job displays this status if it was submitted to a remote processing node for processing but the processor node has a local drive that has the same drive letter as one used by the case associated with the job. For example, the case uses the mapped drive D: for its evidence cache, but the remote processor has its own local drive D: that is not the same as the network-shared D: drive.

Message	Explanation
You cannot rename a Processor Node to [reserved name].	This message displays if you try to rename a processing node to either "Local Machine" or "Next Available." These are reserved names used by EnCase.
Processing crossover preview is not supported. Must acquire and process.	This job status displays if you try to process a crossover preview.

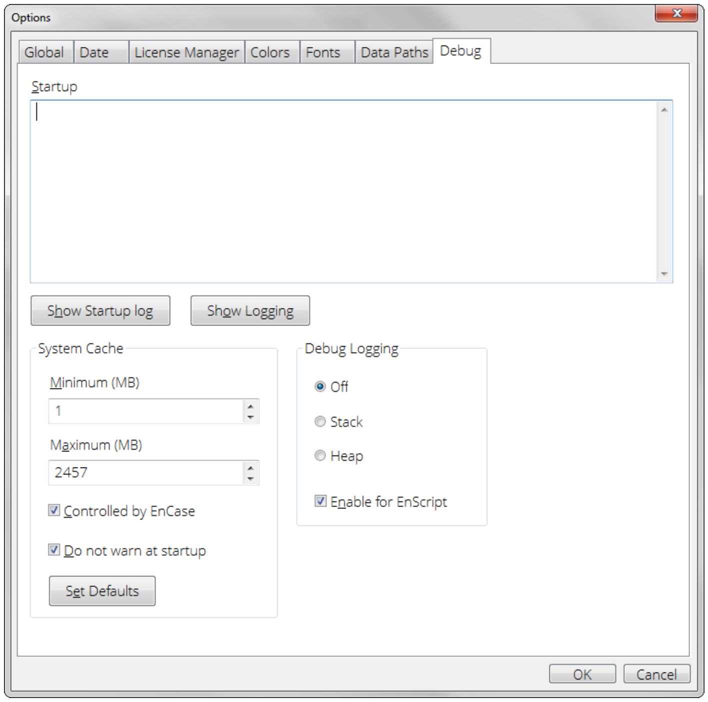
Show Logging

The **Show Logging** option on the **Debug** tab of the Options dialog enables you to view log messages for various operations. The example below shows how to use Show Logging to see Processor Manager trace messages.

Processor Manager Trace Messages

To enable Processor Manager trace messages:

1. Click **Tools** > **Options**.
2. The Options dialog displays. Select the **Debug** tab, then click **Show Logging**.



3. The Logs dialog displays. Scroll through the Log Tags table and click the **EPMTrace** check-box.
4. Select one of these checkbox options from the Log Message Destinations area:
    - Display in debug output
    - Display in console
    - Write to file

5. Messages showing Processor Manager activity are sent to your chosen Log Message Destination.

Acquiring and Processing Live Previews

To acquire or process a live preview you must first highlight the preview in the **Evidence** tab, then choose the desired action under the Process Evidence menu:

- Process
- Acquire, or
- Acquire and Process

If you choose **Process**, the EnCase Processor Options dialog displays with the preview listed as the Current Item choice in the What to Process section of the dialog. If you choose **Acquire** or **Acquire and Process**, the Acquire Device dialog displays instead and shows the information for the preview.

You can only process preview evidence by the Local Machine processor node; therefore, Local Machine must be present in your processor node list to process previews. Some types of live previews have additional restrictions or require user actions before they can be acquired or processed. The section below discusses each type of preview and what restrictions apply, if any.

Live Previews of Local Devices

There are no additional restrictions. You can add any number of acquisition and processing jobs for local previews to the job queue.

Direct Network Previews

You can only queue one direct network preview job at a time. It must finish processing before you can queue another one. Furthermore, you must not be viewing any of the preview data at the time you queue the direct network preview job. If you have viewed any of the preview evidence, you must close all case tabs (Entries, Artifacts, Results, Search, Bookmarks, etc.) before you can queue a job for the direct network preview. Lastly, you cannot add a direct network preview into your case while another direct network preview is being acquired or processed. The recommended workflow for direct network previews is to first acquire the preview to an evidence file, and then process the evidence file.

Crossover Previews

Processing of crossover previews is not supported. You must first acquire the crossover preview to an evidence file and then process the evidence file.

CHAPTER 7

BROWSING AND VIEWING EVIDENCE

Overview	195
The EnCase Interface	195
Filtering Your Evidence	215
Conditions	218
Browsing Through Evidence	223
Viewing Evidence	227
Macintosh Artifacts	230
Viewing Processed Evidence	236
Viewing Email	238

Overview

After creating a case and adding evidence, you can browse and manipulate your views of the evidence in a wide variety of ways:

- You can search through processed evidence quickly, after it is indexed.
- The Gallery view provides thumbnails of images.
- Conditions cull down the viewed data into a manageable subset.
- Filters enable you to eliminate data based on a wide variety of attributes.
- You can browse through evidence directly from evidence files or devices.

This chapter provides an overview of the EnCase interface and describes the ways you can browse and view collected evidence.

The EnCase Interface

The EnCase layout has three sections:

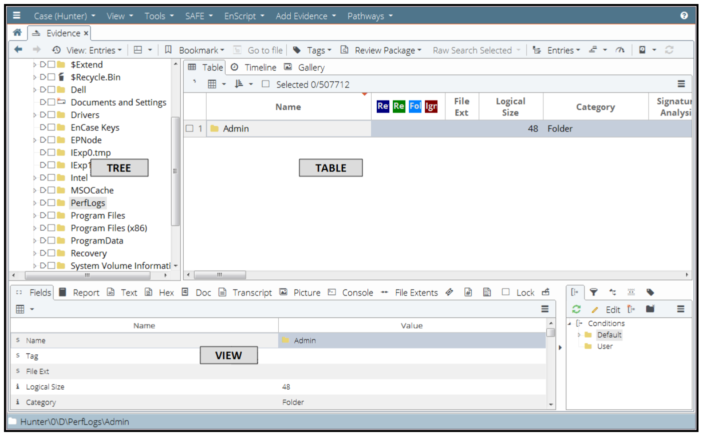
- Tree pane
- Table pane
- View pane

Selections in the Tree pane affect the Table pane. Selections in the Table pane affect the View pane.

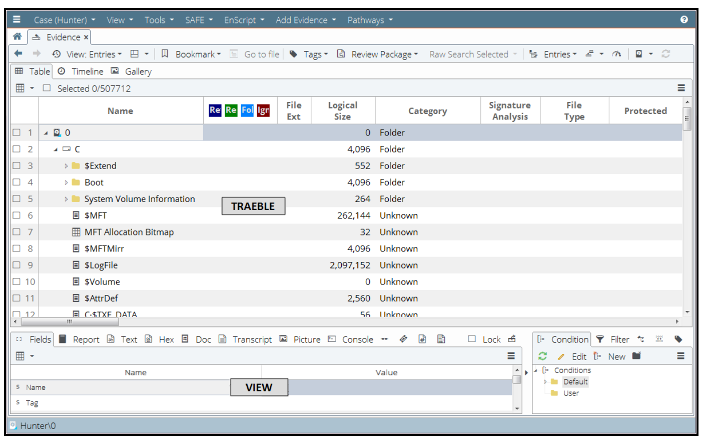
- See Navigating the Tree Pane on page 197 for more information about the Tree pane.
- See Navigating the Table Pane on page 198 for more information about the Table pane.

You can change the way the panes of the screen are configured with the **Split Mode** button:

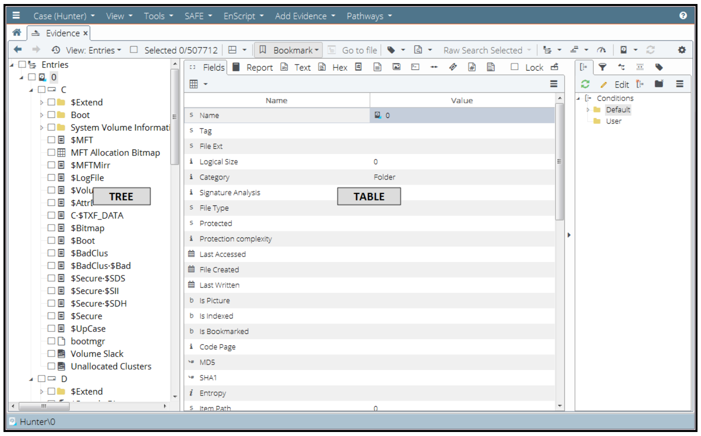
The **Tree-Table** view shows the Tree pane on the left, the Table pane on the right, and the View pane on the bottom. This is the traditional EnCase entries view.



The **Traeble** view combines the Tree and Table panes on the top, and retains the View pane on the bottom. The view provides the ability to browse the folder structure in the Name column.



The **Tree** view displays the Tree pane on the left and the View pane on the right. There is no Table view. This is the suggested view for looking at email artifacts.



Navigating the Tree Pane

The Tree view presents the evidence in a standard hierarchical folder structure. Only evidence files and the folders contained in them display in this view. Individual files display in the Table pane (discussed later). You can use the arrows to expand and contract the tree structure, just as in Windows Explorer.

EnCase uses three methods used to focus on specific files or folders. These methods have different purposes:

- Highlight a folder to display entries in that folder in the Table Pane.
- Click the Set Include icon next to a folder name to display all the entries, files, and sub-folders for that folder in the Table Pane. This overrides the highlighting option.
- Click a checkbox next to an item in any view to select that item for an action, such as an analysis or keyword search. This is sometimes called "blue checking" an item.
    - EnCase displays the number of currently selected items in the Selected box above the Table pane.
    - To clear all selected entries, clear the blue check from the Selected box.

Blue checks persist within a case. Blue checks are case specific and remain persistent in the same tab where they were created.

Blue checks persist when:

- Navigating from Evidence view to Entry view or from Entry view to Evidence view.
- Navigating from Entry view to Record view (for example, viewing file structure on an entry).
- Navigating from Entry view to Results view.
- Navigating from Results to Entry (within the same tab).

By default, blue checks do not persist if you end your session in EnCase.

An option in the **Tools** > **Options** menu gives you the choice to allow blue checks to persist after closing a case or exiting EnCase. This affects performance--it may take longer to open a case if you select this--depending on how many blue checks are active when you close the case.

Blue checks do not persist on evidence removed from a case.

Navigating the Table Pane

The Table Pane is visible in the Tree-Table view. The selection in the Tree pane determines what displays in the Table pane. See Navigating the Tree Pane on the previous page for the various ways to select folders and files.

See Working with Columns on page 200 for information on column management.

The Table pane includes columns with information about the displayed entries.

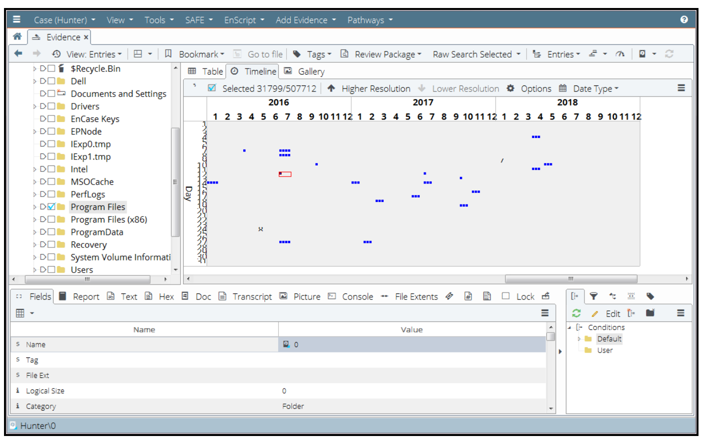
- **Name** is the file/folder/volume, etc., in the evidence file.
- **Tag** displays the tag(s) placed by you on an entry.
- **File Ext** is the entry's extension, which initially determines whether this entry displays in the Gallery view.
- **Logical Size** specifies the file size as the operating system addresses the file.
- **Item Type** identifies the type of evidence, such as Entry (file or folder), Email, Record, or Document. This column is hidden by default.
- **Category** indicates the category of the file from the File Type table.
- **Signature Analysis** displays the results of a file signature analysis.
- **Signature** displays the signature of a Match or an Alias (a renamed extension) resulting from the signature analysis.
- **Protected** indicates if the file is identified as encrypted or password protected during evidence processing.
- **Protection Complexity** provides details on the file's protection.
- **Last Accessed** displays the last date/time the file was accessed. This typically reflects the last time the operating system or any compliant application touched the file (such as viewing, dragging, or right clicking). Entries on FAT volumes do not have a last accessed time.
- **File Created** typically reflects the date/time the file/folder was created at that location. A notable exception to this is the extraction of files/folders from a ZIP archive. Those objects carry the created date/time as they existed when the objects were placed in the archive.
- **Last Written** reflects the date/time the file was last opened, edited, and then saved. This corresponds to the Modified time in Windows.

- **Is Picture** indicates whether the file is an image.
- **Is Indexed** indicates whether the item was indexed during processing.
- **Code Page** displays the character encoding table upon which the file is based.
- **MD5** displays a 128-bit value for a file entry generated by a hash analysis process.
- **SHA1** displays the SHA1 hash value for a file entry generated by a hash analysis process.
- **Entropy** displays the entropy value for a file entry generated by the entropy analysis process.
- **From** displays the sender of the email message. This column is hidden by default.
- **Recipient** displays the receiver of the email message. This column is hidden by default.
- **Primary Device** displays the primary device used. This column is hidden by default.
- **Item Path** identifies the location of the file within the evidence file, including the evidence file name and a volume identifier.
- **Description** describes the condition of the entry: whether it is a file or folder, deleted, or deleted/overwritten.
- **Is Deleted** indicates if the entry is deleted.
- **Entry Modified** indicates when the administrative data for the file was last altered for NTFS and Linux.
- **File Deleted** displays the deleted date/time if the file is in the Recycle Bin's Info2 file.
- **File Acquired** is the date and time the evidence file where this entry resides was acquired.
- **Initialized Size** indicates the size of the file when it is opened. It applies only to NTFS and exFAT file systems.
- **Physical Size** specifies the size of the storage areas allocated to the file.
- **Starting Extent** identifies the starting cluster of the entry.
- **File Extents** displays the cluster fragments allocated to the file. Click in this column for an entry, then click the **File Extents** tab in the View pane to see the cluster fragments.
- **Permissions** shows security settings of a file or folder in the View pane.
- **Physical Location** displays the number of bytes into the device at which the data for an entry begins.
- **Physical Sector** lists the sector number into the device at which the data for an entry begins.
- **Evidence File** displays where the entry resides.
- **File Identifier** displays an index number for a Master File Table (NTFS) or an Inode Table (Linux/UNIX).
- **GUID** indicates the Global Unique Identifier for the entry, to enable tracking throughout the examination.
- **Hash Set Names** displays the Boolean value as true if a file belongs to one or more hash sets. This column is hidden by default.
- **Short Name** displays the name Windows gives the entry, using the DOS 8.3 naming convention.
- **VFS Name** displays the name for files mounted with the EnCase Virtual File System (VFS) module in Windows Explorer. This replaces the Unique Name column in previous versions of EnCase.

- **Original Path** displays information derived from data in the Recycle Bin. This column shows where files in the Recycle Bin originated when they were deleted. For deleted/overwritten files, this column shows the file that overwrote the original.
- **Symbolic Link** displays data equivalent to a Windows Shortcut in Linux and UNIX.
- **Is Duplicate** displays True (Yes) if the file is a duplicate of another.
- **Is Internal** indicates if the file is an internal system file, such as the $MFT on an NTFS volume.
- **Is Overwritten** indicates if the first or more clusters of an entry were overwritten by a subsequent object.

Viewing Information in a Timeline

The Timeline view shows patterns of different types of dates and times. Zooming in lets you see time in a more granular way (up to a second-by-second timeline). Zooming out provides a larger overview (up to a year-by-year timeline).



Timeline view options allow you to see data in ranges of weeks, days, hours, and minutes. The maximum number of weeks displayed is 104. The maximum number of minutes displayed is 1440.

Working with Columns

To rearrange table columns in any order, click and drag a column heading and drop it into a new location.

To sort by a column, double click the column heading. To institute a subsort, hold down the Shift key and double click the column heading. You can sort columns up to five layers deep.

You can lock columns on the left side of the Table pane so they remain visible when scrolling horizontally.

- To lock a column, click anywhere in the column and select **Column > Set Lock** from the arrow dropdown menu on the right of the Table pane. The selected column and all columns to its left are now locked.
- If columns are rearranged, all columns to the left of that position remain locked.
- To release the lock, click anywhere in the column and select **Column > Unlock** from the arrow dropdown menu on the right of the Table pane.

You can enable or disable individual columns by selecting **Column > Show Columns** from the arrow dropdown menu on the right side of the Table pane.

COLUMNS IN SEARCH RESULTS AND BOOKMARK VIEWS

The list below shows additional columns available in the Search Results and Bookmark column views. You can sort these columns like any other columns in EnCase. You must enable these columns to include them in a view.

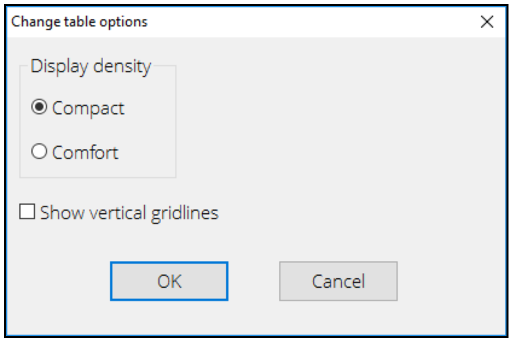
- Received (the time an email was received as identified by the email application)
- Sent (the time an email was sent as identified by the email application)
- Description (File, Archive, etc.)
- Action URL
- Icon URL
- Requesting URL
- URL Host
- URL Host Name
- URL Name
- True Path
- Item Path
- Symbolic Link
- Entry Modified
- Has Attachments

Adjusting Spacing in a Table

You can adjust how tightly together rows are spaced within a table.

Click the hamburger menu icon at the far right of the table, then select **Change Table Options**. From the dialog, select the display density you prefer. There are two options: compact and comfort.

Select **Show vertical gridlines** to add more visual structure to the table.



Viewing Content in the View Pane

You can view information about a device or entry in a variety of ways in the EnCase View pane. The **Evidence**, **Results**, and **Artifacts** tabs have slightly different viewing options, but operate in generally the same manner.

By default, EnCase uses the appropriate viewer for each item selected whenever possible. To keep the tabs from switching for different data types, click the **Lock** checkbox on the top right of the View pane to lock the view to that tab.

The lower View pane provides several ways to view file content:

- The **Fields** tab displays all information available regarding an item. All fields shown on this tab are indexed.
- The **Report** tab provides a readable, formatted view of metadata. This is the preferred view for email.
- The **Text** tab displays files in ASCII or Unicode text.
    - You can modify how text in this tab displays. See Changing Text Styles on page 204.
    - When viewing search results, select **Compressed View** in the **Text** tab to see only lines with raw keyword search hits.
    - Use the **Previous/Next Hit** buttons to move through hits in the file. If there are no more hits in the file, the next item opens and the first hit is found.
- The **Hex** tab displays files as straight hexadecimal.
    - When viewing search results, select **Compressed View** to see only lines with raw keyword search hits.
    - Use the **Previous/Next Hit** buttons to move through hits in the file. If there are no more hits in the file, the next item opens and the first hit is found.

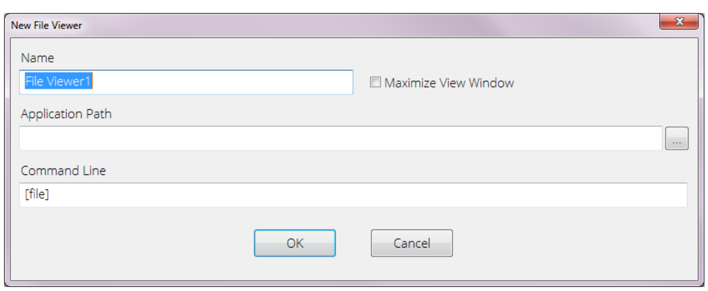
- The **Doc** tab provides native views of formats supported by Oracle Outside In technology.
- The **Transcript** tab displays the same formats as the **Doc** tab, but filters out formatting, allowing you to view files that cannot display effectively in the **Text** tab.
  - The **Transcript** tab displays the extracted text from the file.
  - When viewing search results, select **Compressed View** to see only lines with index query hits.
  - Use the **Previous/Next Hit** buttons to move through hits within the file. If there are no more hits in the file, the next item opens and the first hit is found.
- The **Picture** tab displays graphics files. If the highlighted file in the Table pane is an image that can be decoded internally, EnCase lets you select the Picture view in the View pane and displays the image.
- **File extents** shows sector information about the selected file. This works on entry evidence only.
- The **Permissions** tab displays security permissions for a file, including the name and security identification number (SID) of the user(s) who have permission to read, write, and execute a file.
- **Hash sets** shows hash information for entry evidence only.

Adding an External File Viewer

EnCase can display different types of files as they would appear in their native application.

If you encounter a file type that EnCase does not have built-in capabilities to display, you can add an external viewer for that file type.

1. From the **Evidence** tab, right click on an evidence item and select **Open with** > **File Viewers**. The Edit File Viewers list displays.
2. Click **New**. The New File Viewer dialog displays



  - **Name** is the name of the file viewer.
  - Check **Maximize View Dialog** to open the file viewer in a maximized new window.
  - **Application Path** contains the filename and path to the viewer's executable.

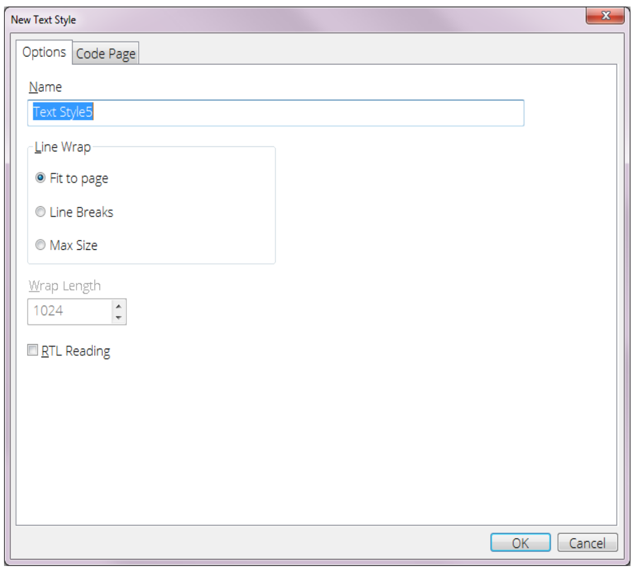
- **Command Line** contains a reference to the executable and any parameters used to customize the viewer.

3. Click **OK**. The new file viewer displays in the Edit File Viewers list for you to use as needed.

Changing Text Styles

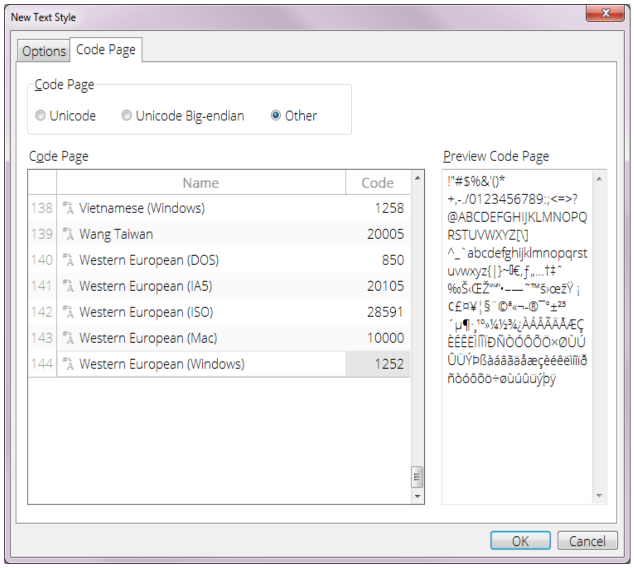
In the **Text** or **Hex** tabs, you can apply different viewing styles to display the text in configurations that assist in viewing particular types of data. To change the style select the **Text Styles** menu from the **Text** or **Hex** tabs in the View Pane.

1. Click **New** to create a new text style. The New Text Style dialog displays.



- **Name** is the name of the text style.
- **Fit to page** eliminates line breaks in displayed content, and displays all text in the window.
- **Line Breaks** displays line breaks in the content.
- **Max Size** ignores line breaks in the content, and wraps lines at the value set in Wrap Length.
- **Wrap Length** specifies the length where a line break occurs. When you select Max Size, line breaks occur only at the value of this setting.
- **RTL Reading** sets the text display to read right-to-left (RTL).

2. Click the **Code Page** tab to select the code page.



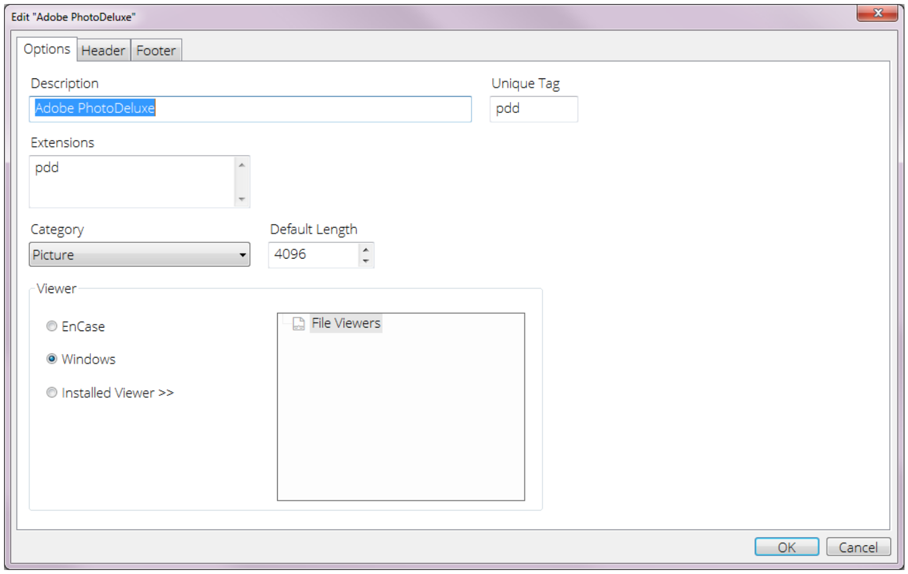
- **Unicode** specifies little-endian Unicode. If you use UTF-7 or UTF-8, select **Other**, not Unicode.
- **Unicode Big-Endian** specifies big-endian Unicode.
- **Other** lets you select from the Code Page list.
- **Code Page** contains a list of supported code pages.

3. Click **OK** to save the new text style and return to the Edit Text Styles dialog.
4. Click **OK** to make the new style available. The new text style is now applied to the **Text** tab in the View pane.

Associating File Types with a File Viewer

When you add a new file viewer to EnCase, you can associate it with a file type.

1. On the **Evidence** tab, select **View** > **File Types**. The **File Types** tab displays.
2. Double click the file type you want to associate the new viewer with.
3. The Edit File type dialog displays.



- **Description** is the file type to associate with the file viewer.
- **Extensions** is a list of file types to associate with the file viewer.
- Select a **Default Length** to determine the end of the file.
  - This is used if a footer for the file type is not specified and is used to determine the length of the file.
  - If this is not set, EnCase uses a default length of 4096 bytes to determine the end of the file.
  - Longer lengths are recommended for pictures and ZIP files.

- The **Viewer** area contains options for selecting the type of viewer to use:
  - Click **EnCase** to associate the built-in EnCase viewer with the file type you define.
  - Click **Windows** to associate Windows with the file type you define.
  - Click **Installed Viewer** to associate an installed viewer with a file type. Use the installed viewers tree to select the specific viewer.

- The **Installed viewers tree** lists the file viewers currently known to EnCase.

4. Click **OK**. All files of this file type are now associated with the selected file viewer.

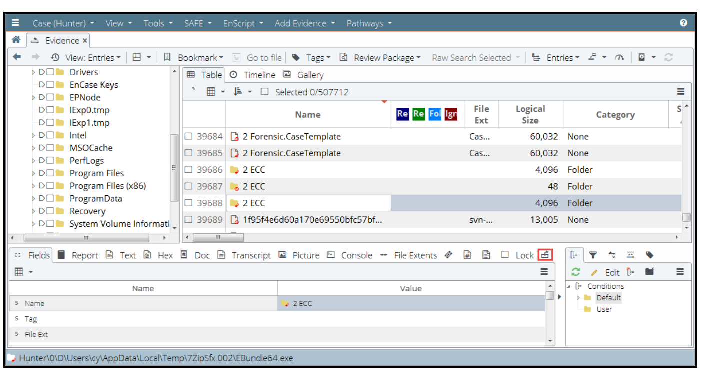
Viewing Decoded Data

You can see decoded interpretations of your evidence, when viewing it in text or hex format, using the **Decode** tab in the lower right pane of the **Evidence** pane.

1. On the **Text** or **Hex** tabs in the **View** pane, select the bytes you want to decode.
2. Click the **Decode** tab in the lower right pane and select from the list of decoding options.
3. View the decoded interpretations of your evidence:
    - The Quick View decoder enables you to view common decode interpretations in one screen.
        - When populating the Quick View table, all bytes required to successfully interpret the data are read.
        - For example, if one byte is selected, and four bytes are required to decode a 32-bit integer, Quick View looks at the next three bytes to provide the decoded interpretations.
    - The View Types list displays specific decoded values, organized in a tree structure.
        - With the exception of pictures, when viewing by Type, only the selected bytes are interpreted.
        - For example, if one byte is selected, and four bytes are required to decode a 32-bit integer, a decoded interpretation is not available.
        - EnCase Forensic attempts to decode pictures from the selected starting byte. The bytes for the entire picture do not need to be selected.
4. To bookmark your selection:
    - From Quick View, right click and select **Bookmark**.
    - From the View Types list, click the **Bookmark** button.

Undocking the View Pane

You can undock the View pane in order to place it elsewhere on your desktop. To undock the View pane, click the Undock icon in the upper right corner of the View pane. The Filter/Conditions pane moves with the View pane.

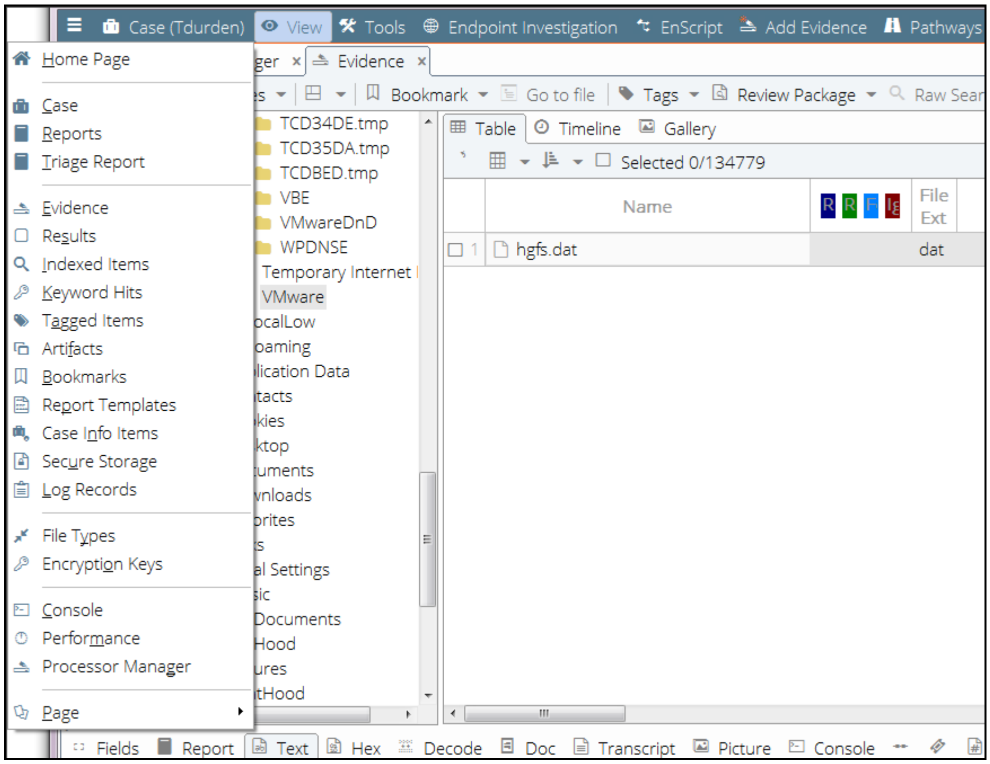


To return the View pane to the main window, close the View pane window.

Using Views/Tabs

The **View** menu provides a variety of views of your information.

Clicking these views opens a new tab in the EnCase window.



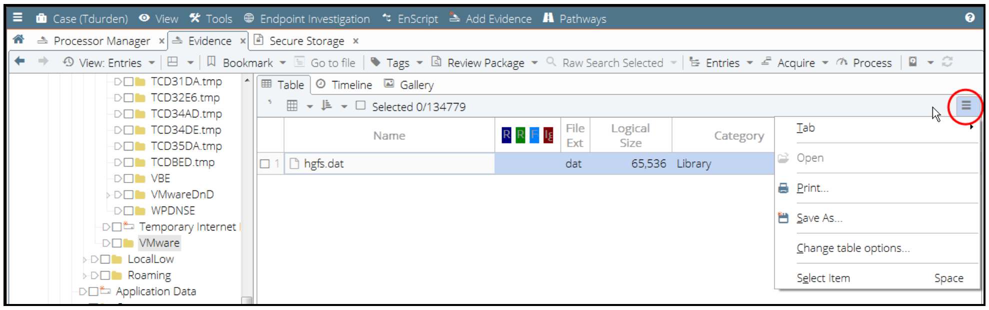
Secure Storage: Add Local User

To add a local user:

1. Click **View** > **Secure Storage**.
2. In the **Secure Storage** tab Table pane, click the hamburger menu at the far right, then click **User List** in the dropdown menu.
3. Right click in the body of the **Local Users** tab and select **New**.
4. In the Local User dialog, enter the name and SID of the new user. You can optionally enter a comment.
5. Click **OK**.

Right Hamburger Menu

The hamburger dropdown menus on the right side of the menu bar of each pane provide generic functions, such as printing, saving, sorting, and managing columns.

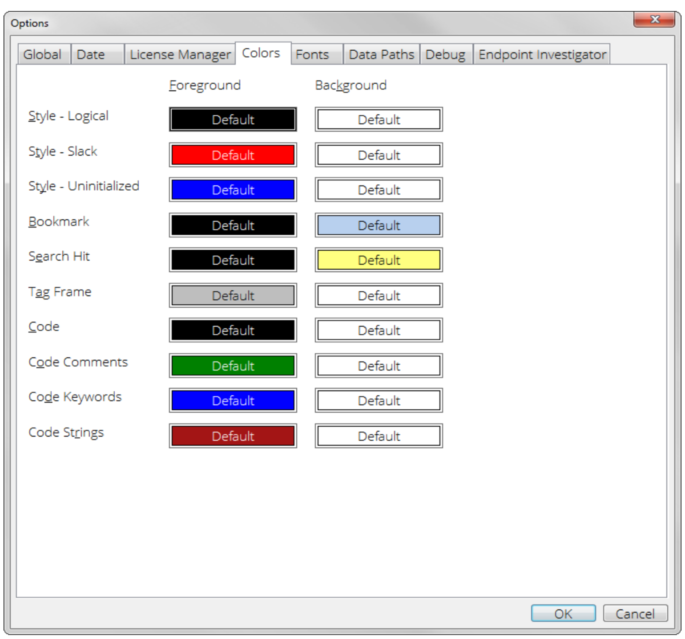


Changing Text Color

You can change the way various types of text display in EnCase. This is useful if, for example, you want to change the way the uninitialized area of a file displays and differentiate it from the logical size of the file.

To change the color display of text:

1. From the **Tools** menu, select **Options**.
2. In the Options dialog, click the **Colors** tab.



3. To change the color of the text, right click the **Foreground** color and select the new color from the dropdown menu. If the color you want is not an option, double click the foreground color and select from the color palette.
4. To change the background color, right click the **Background** color and select the new color from the dropdown menu. If the color you want is not an option, double click the foreground color and select from the color palette.
5. Click **OK**.

Navigating the Evidence Tab

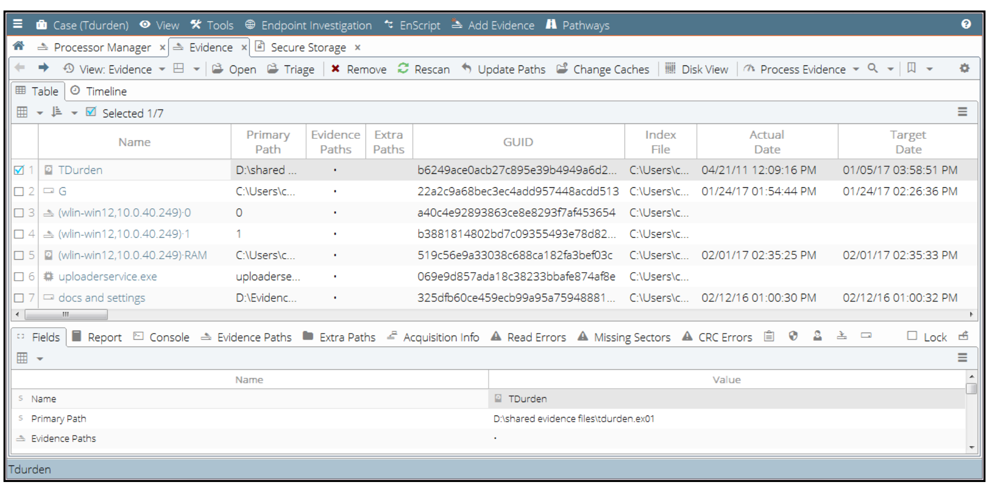
When browsing and viewing your evidence, much of your time is spent in the **Evidence** and **Artifacts** tabs.

Evidence is information you can view and process in EnCase from a variety of sources:

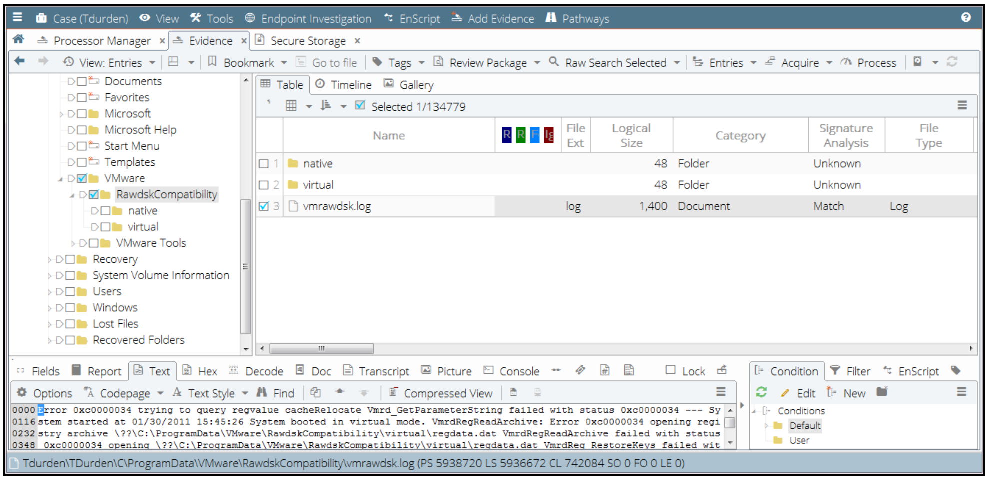
- `.Ex01`, `.Lx01`, `.E01`, and `.L01` files
- `VMDK` files
- `VHD` files
- Raw `DD` Image files

EnCase parses these files as they come in. Each file displays as a device on the interface. All parsed data from a device is stored in a device cache so it does not need to be reloaded each time it is viewed.

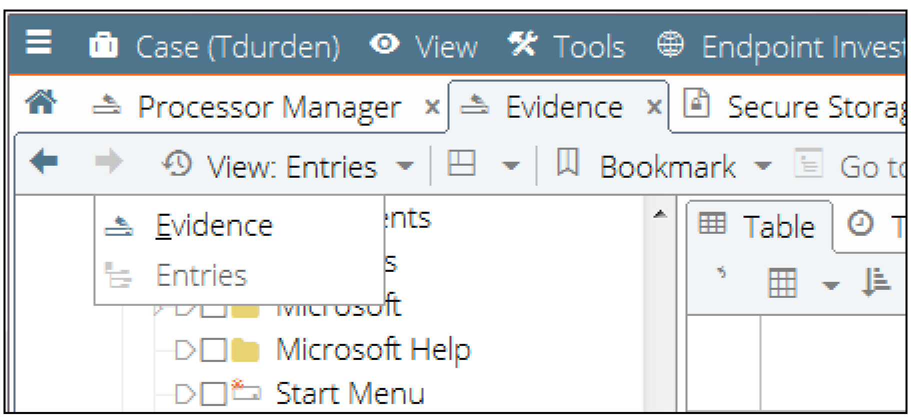
The **Evidence** tab table view shows the evidence currently loaded into your case. Notice that when you are viewing a list of evidence the **View** button displays as **View: Evidence**.



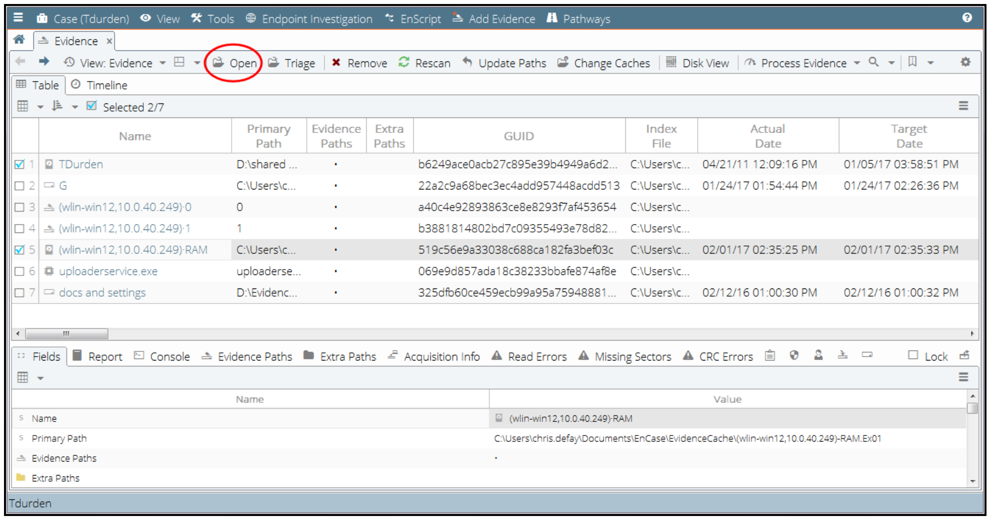
Click any one of these pieces of evidence to open it more fully. Notice that when you are viewing an expanded view of an entry, the **View** button displays as **View: Entries**.



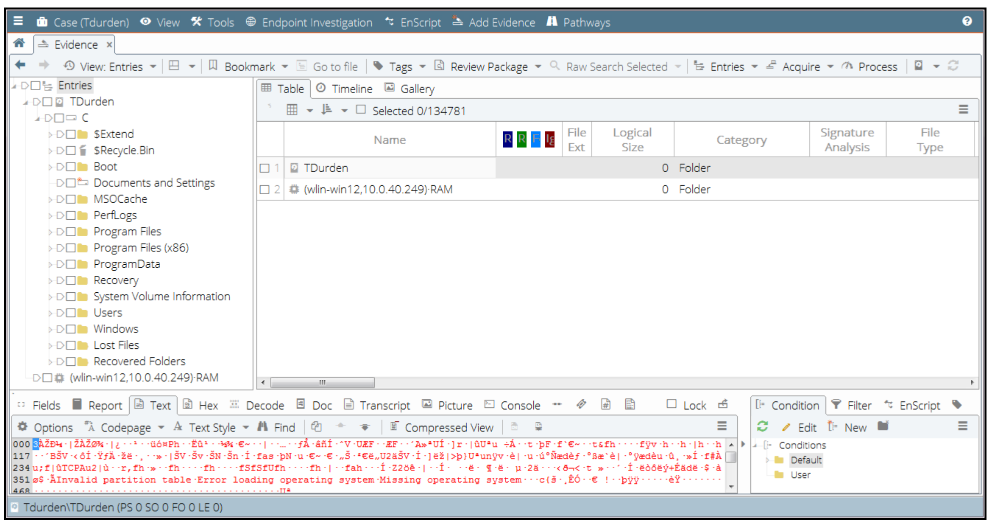
Click the **View** button to move between the top level list of devices or see an expanded view of specific evidence:



If you want to see all the evidence expanded into the same entry screen, go to the top level list of devices, select all the evidence files you want to see, and click **Open** from the menu:

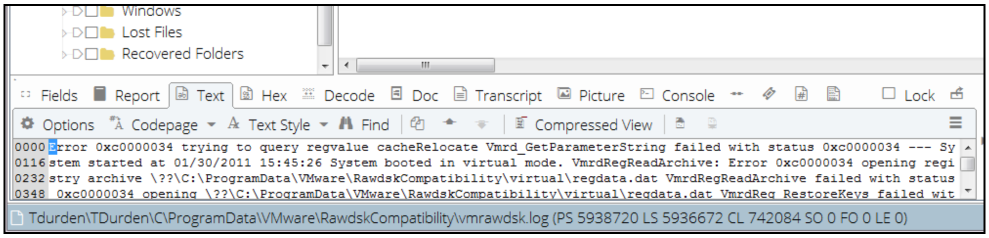


The display changes to show the expanded view of all selected evidence entries.



The status bar at the bottom of the screen displays the full path of the highlighted item. This can be useful when documenting the location of evidence found in unallocated space. If a deleted/overwritten file is highlighted, it indicates the overwriting file.

Specific sector, cluster, and file information is presented in parentheses after the file path of the selected item.



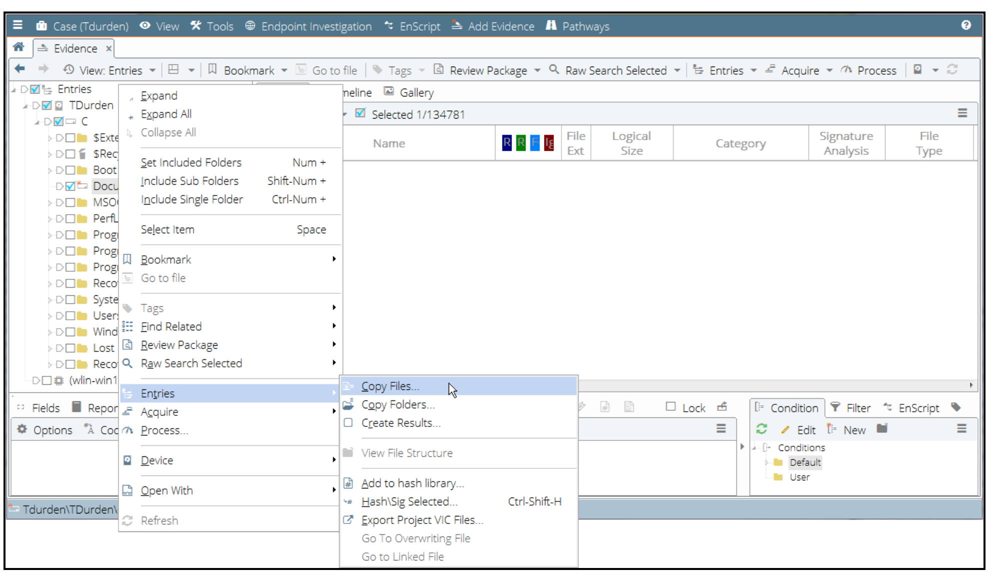
The status bar provides additional details about the file.

Abbreviation	Definition
PS	physical sector number
LS	logical sector number
CL	cluster number
SO	distance in bytes from the beginning of the sector (sector offset)
FO	distance in bytes from the beginning of the file (file offset)
LE	number in bytes of the selected area (length)

The status of any processing activity displays in the lower right of the status bar.

Entries View Right Click Menu

In Entries view, right click any entry in the tree, then position the cursor over **Entries** to display the Entries submenu.



- **Copy Files** opens the Copy Files dialog.
- **Copy Folders** opens the Copy Folders dialog.
- **Create Results** opens the Create Results dialog.
- **View File Structure** opens the View File Structure dialog.
- **Add to hash library** opens the Manage Hash Library dialog.
- **Hash\Sig Selected** opens the Hash\Sig Selected dialog.
- **Export Project VIC Files** generates a .JSON file for export to Project VIC.
- **Go To Overwriting File**: If a file is overwritten, this option takes you to the overwriting file.

Viewing Data on a Device

Using Disk view, you can view files and folders in terms of where the data appeared on the media. You can also see placement of clusters and/or sectors and fragmentation of files.

Disk view is available from the **Entry** view of the **Evidence** tab. To open Disk view, select **Disk View** from the **Device** menu.

- The file selected in the table is highlighted in Disk view as dark blue squares.
- Allocated sectors display in light blue.
- Unallocated sectors display in gray.

Select **Auto Extents** to automatically highlight all the remaining extents that make up the file associated with the selected sector. If **Auto Extents** is off, double click a sector to show the remaining associated extents.

Click the **Evidence** tab to return to entries.

Changing Evidence Cache Location

EnCase provides a wizard that steps you through the process of changing the location of your evidence cache.

To change the location of your evidence cache:

1. In the **Evidence** tab toolbar, click **Change Caches**. The Change Caches dialog displays.
2. To use the base Case folder for the primary evidence cache, select the corresponding checkbox.
3. To change the location of the primary evidence cache, click the Primary evidence cache **ellipsis button**, browse to the new location, and click **OK**.
4. To add a secondary evidence cache location, click the Secondary evidence cache **ellipsis button**, browse to the new location, and click **OK**.

5. Click **Next**. The Evidence Cache Preview dialog displays. Status is listed for each evidence cache:
    - **Ready (Primary)** means the new path contains a cache in the primary cache.
    - **Ready (Secondary)** means the new path contains a cache in the secondary cache.
    - **Missing** means the old location had a cache, but neither the primary nor secondary locations have a cache for the evidence.
    - **None** means there never was a cache for this device.

5. Click **Finish**. If any evidence items have a status of missing, a message displays informing you that a new evidence cache will be created for the missing evidence items. To proceed, click **Yes**.

Navigating the Artifacts Tab

The **Artifacts** tab displays the inner structure of compressed files or other files that require additional processing to be viewed. This includes email archives, .ZIP, .RAR files, Internet artifacts, output for EnScript modules, mobile device data, etc.

All artifacts available in the case can be seen in the root of the **Artifacts** tab. Click **View > Artifacts** to browse this list. These artifacts are grouped by evidence file, then by type. Click the blue link to open a single artifact. Blue check artifacts and click **Open** in the toolbar to open multiple artifacts in one view.

You can also access artifacts from the Entries view. Entries that you can expand and view in the **Artifacts** tab display as blue links marked with a green plus sign in the Entries view.

If an entry does not display as a blue link, select it and click **View File Structure** from the **Entries** dropdown menu. The View File Structure command automatically expands, or mounts, the file. After initially mounting the file, you can see the expanded data in the **Artifacts** tab as well.

Filtering Your Evidence

Filters are EnScripts that provide a table view of all entries matching a particular set of criteria. Filters do not remove any items from the case. They simply specify which entries display in the Table pane.

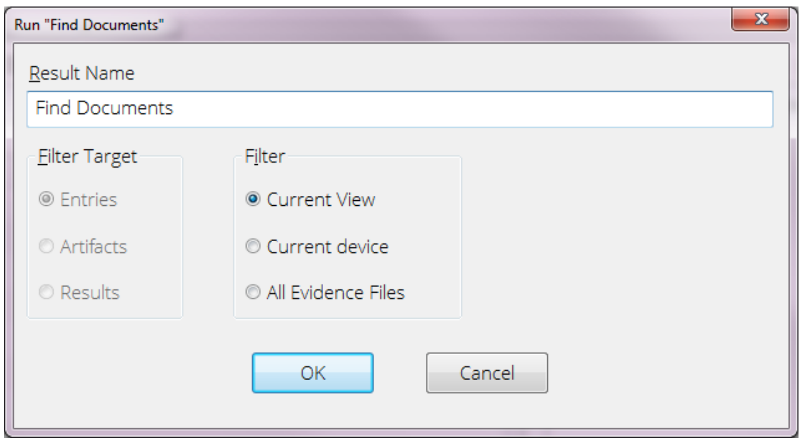
Depending on the currently selected tab, different types of filters are available. For example, the filters available for search hits are different from those available for entries.

Both filters and conditions work the same way in terms of how they affect the items in the Table pane.

Running an Existing Filter

EnCase comes with a number of preconfigured default filters.

1. From the lower right pane, open the **Filter** tab. The preconfigured filters are in the Default folder.
2. Double click the filter you want, then click **Open**. A Run Filter dialog displays.



3. Select the options you require.
    - **Filter Target** specifies what type of case data to filter.
    - **Current View** filters the items that are in the current view, and displays the results in that view.
    - **Current device** filters all items in the current device, and displays the results in a Result Set.
    - **All Evidence Files** filters all items in all evidence in the case, and displays results in a Result Set.
    - **Result Name** is the name of the Result Set, if applicable.

4. Click **OK** to run the filter. Depending on which filter you selected, additional dialogs may display. When a filter is running, the name of that filter shows in the lower right of the status bar. When complete, the results display in the specified result location.

Creating a Filter

In addition to using the filters already provided, you can create your own filters.

> **Note:** You need a working knowledge of EnScript to make a new filter. If you do not have this working knowledge, you may be able to create a condition to perform the same function.

1. From the **Filter** tab, select **New** from the toolbar. The New Filter dialog displays.
2. Enter a new name for the filter, if desired.
3. Click **OK**. The **New Filter** tab displays, showing a source editor.
4. Enter EnScript code as required to accomplish your task. The newly created filter displays at the bottom of the filters list.

Editing a Filter

To change an existing filter's behavior, edit it.

1. Open the **Filter** tab in the lower right pane. A list of all customized and preconfigured filters displays. You may only edit customized filters.
2. Select the filter you want to edit and click **Edit**. The source code opens in a **Filter** tab.
3. Edit the code as needed.

To change the name of an existing filter, right click the filter in the **Filter** tab and click **Rename**.

You may only edit customized filters. To edit a preconfigured filter, it must first be copied to the User folder. Drag the filter to the desired folder while holding the control key or drag using the right mouse button to make a copy. The copy may then be edited.

> **Note:** Preconfigured filters cannot be edited because they may be updated by future versions of EnCase.

Deleting a Filter

Default filters are read-only and you cannot modify or delete them. However, you can delete any custom filter you created.

To permanently delete a filter:

1. Open the **Filter** tab in the lower right pane.
2. Right click the filter you want to delete, then click **Delete**.
3. Click **Yes** to confirm the deletion.

Sharing Filters

You can share your own filters, and use filters created by other EnCase users.

1. Open the **Filter** tab in the lower right pane. A list of all customized and preconfigured filters displays.
2. Right click the filter you want to export, then click **Browse**. A Windows Explorer window opens.
3. Copy the appropriate filter.
4. Navigate to the place where you want to store the file and click **Paste**.
5. To import a filter created by someone else, use **Browse** to view the User folder in Explorer, and place the new filter in that folder.

Conditions

Conditions are compilations of search terms that instruct EnCase to find certain data based on a certain property of information.

Conditions are similar to filters in that they display only those entries matching a specific set of criteria in the Table pane. Both conditions and filters are EnScript code that performs a filtering process on your data.

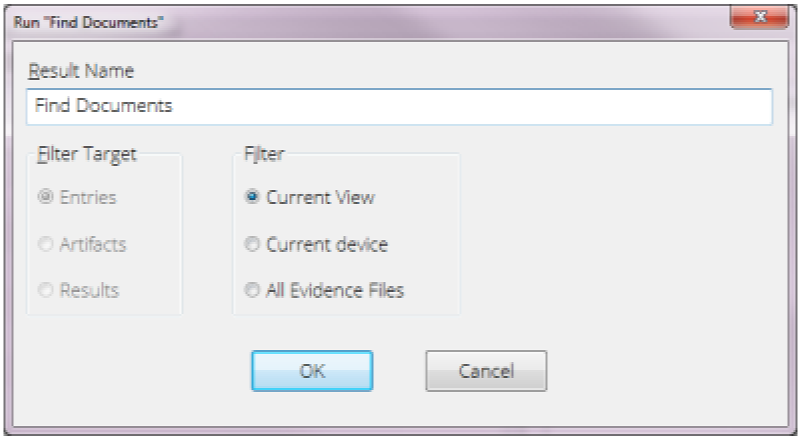
The difference between filters and conditions is that creating a condition does not require that you can program in EnScript. Through a special interface you can create them without coding directly in EnScript.

Once you create a condition, you can run it on any evidence in the case.

Running an Existing Condition

EnCase comes with a number of preconfigured default conditions.

1. From the lower right pane, open the **Condition** tab. The preconfigured conditions are in the Default folder.
2. Double click the filter you want to display the Run Condition dialog.

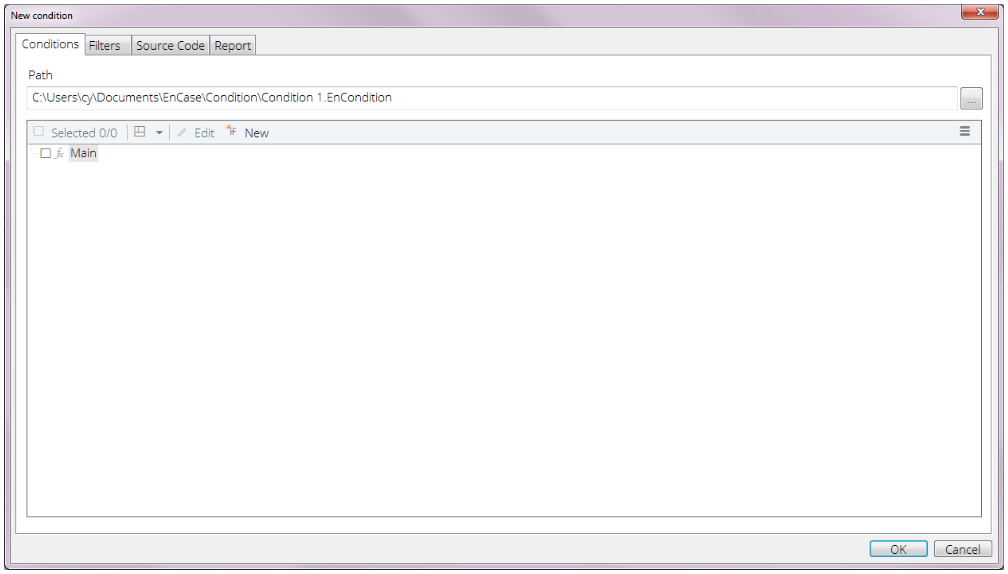


3. Select the options you require.
    - **Filter Target** specifies what type of case data to filter.
    - **Current View** filters the items that are in the current view, and displays the results in that view.
    - **Current device** filters all items in the current device, and displays the results in a Result Set.
    - **All Evidence Files** filters all items in all evidence in the case, and displays results in a Result Set.
    - **Result Name** is the name of the Result Set, if applicable.

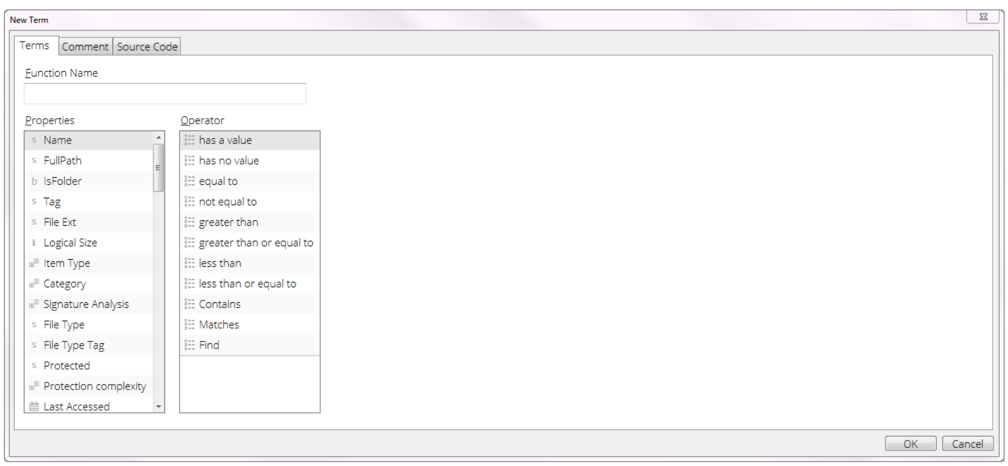
4. Click **OK** to run the condition. Depending on which condition you selected, additional dialogs may display. When a condition is running, the name of that condition shows in the lower right of the status bar. When complete, the results display in the specified result location.

Creating a New Condition

1. From the **Condition** tab, select **New** from the toolbar. The Condition dialog displays.



2. Enter a new name for the condition, if desired.
3. Right click the **Main** function node on the conditions tree and select **New**. The New Term dialog displays.



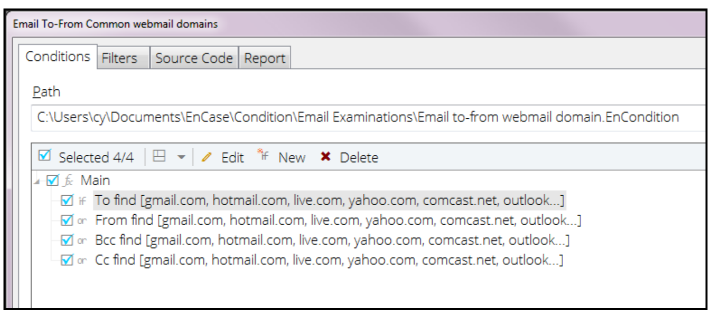
- Select a property, an operator, and, if appropriate, a value and choice.
  - Properties allow you to specify what information you want to filter.
  - Operators indicate how you want to filter the information. Operators that allow you to enter values can use GREP expressions, or provide a list of values to find.

    - For any condition using a literal comparison (such as Matches), make sure there are no spaces at the end of any value string.

  - To edit the source code directly, click **Edit Source Code**.
  - To nest terms, create a folder by right clicking on the parent condition folder in the Tree pane and choosing **New Folder**. Place the nested terms inside the parent folder.
  - To change the AND/OR logic within the condition, right click the term and select **Change Logic**. This changes the AND operator to an OR, and vice versa.
  - To negate the logic of a term, right click the term and select **Not**.
  - Repeat the steps above to create as many terms as you want to make the condition as detailed as possible.

  Note: The Hash Sets property values display as integers.

4. When you finish, click **OK** to close the New Term dialog. The new condition displays in the Edit condition dialog.
5. Repeat for as many conditions as you need. As you accumulate conditions, make sure they display in the correct hierarchical order for greatest efficiency.



  - When you run the condition, the terms are evaluated in the order in which they display.
  - Conditions work from the top to the bottom, so the sequence in the condition tree directly affects how well the condition works. To be most effective, for example, place an extension search for all .docx files before a keyword search. This saves processing time by not looking for keywords in files that may not even contain text.
    - Folders operate much like parentheses in mathematical problems, in that the folder allows its contents to be grouped together based upon the logic.
    - Logic operators operate on the folder where they display and do not impact the folders above or below them.

  - To nest terms, right click the parent condition folder in the tree and choose **New Folder**. Place the nested terms inside the parent folder.

- To toggle the AND/OR logic within the condition, right click the term and select **Change Logic**. This changes the AND operator to an OR, and vice versa.
- To negate the logic of a term, right click the term and select **Not**.

6. Click **OK** to save and close the dialog.

Editing Conditions

1. Right click the condition you wish to edit and select **Edit** from the menu.
2. The Condition dialog displays.
3. Edit the condition as needed.

To change the name of an existing condition, right click the condition in the **Condition** tab and click **Rename**.

You can only edit customized conditions. To edit a preconfigured condition, first copy it to the User folder. Drag the filter to the desired folder while holding the control key or drag using the right mouse button to make a copy. You can then edit the copy.

> **Note:** You cannot edit preconfigured conditons because they may be updated by future versions of EnCase.

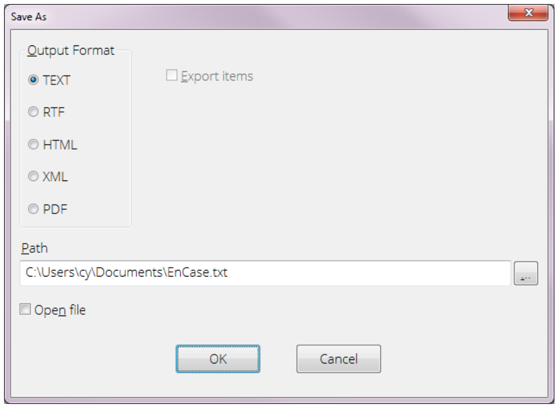
Sharing Conditions

You can share your own conditions, and use filters created by other EnCase users.

1. Open the **Condition** tab in the lower right pane. A list of all customized and preconfigured conditions displays.
2. Right click the condition you want to export, then click **Browse**. A Windows Explorer window opens.
3. Copy the appropriate condition.
4. Navigate to the place where you want to store the file and click **Paste**.
5. To import a condition created by someone else, use **Browse** to view the User folder in Explorer, and place the new condition in that folder.

Printing a Condition

The **Report** tab in the Condition dialog provides a plain text version of the condition. To print or export this report, right click in this tab and select **Save As**. The export dialog provides a variety of options for saving the report.



Browsing Through Evidence

The easiest way to browse through evidence is to view it in either the **Evidence** or the **Artifacts** tab. The **Evidence** tab displays the evidence currently loaded in your case. The **Artifacts** tab displays the inner structure of compressed files or other files that need additional processing to be viewed.

- To browse through Internet artifacts, expand an Internet node in the Tree pane of the **Artifacts** tab. The Browser node contains the various Internet items. Use the **Fields** tab in the lower pane to view the most information.
- To browse through Archives, expand the Archives node in the Tree pane of the **Artifacts** tab and browse through the various Archive items in the Table pane. Use the **Fields** tab in the lower pane to view the most information.
- To view all the results of the modules used for processing evidence, expand the Evidence Processor Modules node in the Tree pane of the **Artifacts** tab and browse through the various items, Use the **Fields** tab in the lower pane to view the most information.
- To view mobile device data, open the evidence file in either the **Artifacts** or **Evidence** tab. The EnCase Mobile Investigator is the best way to view all mobile device information.

Check for Evidence when Loading a Case

When you load a case, EnCase checks for the existence of evidence and displays a status in Evidence view.

Finding the Location of an Evidence Item

When working with search results, the **Go to File** button helps you find the original location of an item of processed data. This is useful for Module results or registry keys that need to be seen in context.

In the table pane, select the item you want to research and click **Go To File**. The view changes to display the device where the entry is located. If you select an email attachment, you are taken into the email file, with the email message containing the attachment selected.

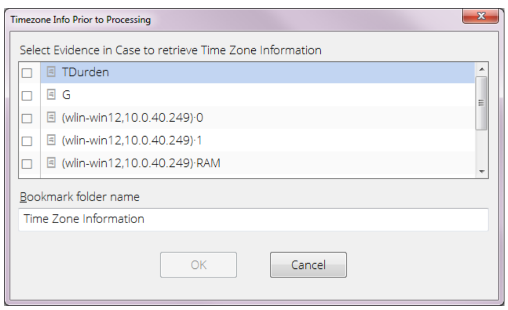
If an item resides in a top level device, the file structure may not display any changes when you click the **Go To File** button, because there are no additional levels above the top level.

Determining the Time Zone of Your Evidence

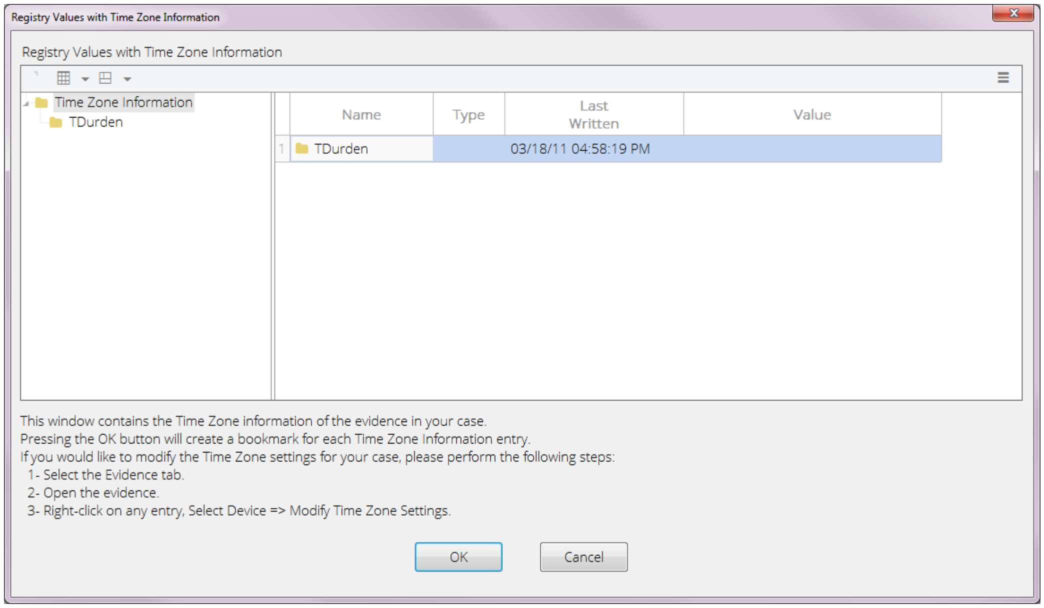
When performing an investigation, you may need to see the registry time zone values associated with your evidence. This must be done before processing the evidence.

To determine the time zone of your evidence:

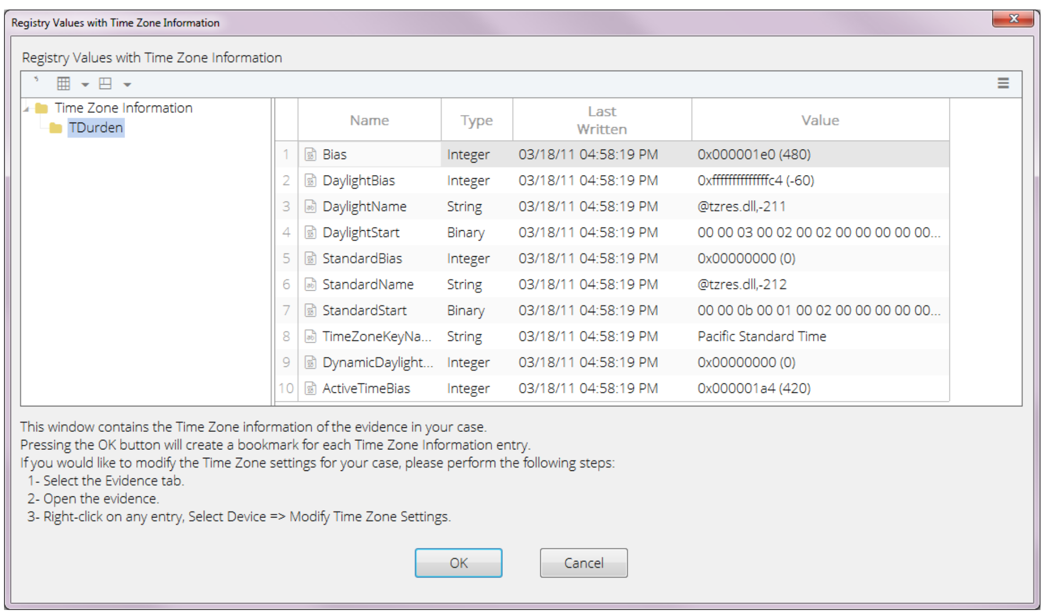
1. On the home page in the Pathways group, click **Full Investigation**.
2. In the Full Investigation dialog, click **Determine the Time Zone of the Evidence**. The Time Zone Info Prior to Processing dialog displays.



3. Select the evidence you want time zone information for, enter a bookmark folder name or accept the default name, then click **OK**.
4. The Registry Values with Time Zone Information dialog displays.



5. In the left pane, click an item in the tree to see detailed time zone information in the right pane.



6. Read the instructions in the dialog if you want to modify time zone settings. Click **OK** to create a bookmark for each time zone entry.

Viewing Related Items

For processed evidence you can find items related by name, time, and hash value. When looking for related items by time, you can select a duration.

1. From the **Evidence** or **Artifacts** tabs, right click the item you want to research, then click **Find Related**.
2. Select whether you want to find related by name or by time.
    - An appropriate dialog displays depending on what you select.
    - If you are finding related information by name, a search dialog displays with index, tag, and keyword options.
3. Click **Save & Run** to run the query. When you finish, the results display in the **Results** tab, under the name of the query.

Browsing Images

The Gallery view of the **Evidence** or **Artifacts** tab provides a quick and easy way to view images. This view is best used when viewing your evidence in a Tree-Table.

By default, images in Gallery view are sorted by extension. You can view image files with incorrect extensions after they are processed using the Evidence Processor.

You can access all images within a highlighted folder, highlighted volume, or the entire case. If a folder is highlighted in the Tree pane, all files in the folder display in the Table pane. Click a folder's **Set Include** to select all files in that folder and files in any of its subfolders. Once selected on the Table pane, any images in the selected files display in Gallery view.

- To reduce the number of images displayed in a row in Gallery view, right click any image, then click **Fewer Columns**.
- To increase the number of images displayed per row in Gallery view, right click any image, then click **More Columns**.
- To bookmark images in Gallery view, right click the image and select the type of bookmark to assign to it.
- To view ownership permissions for an image, select the image and click the **Permissions** tab in the lower pane.

By default, Gallery view displays files based on their file extension. For example, if a .jpg file is renamed to .dll, it does not display in Gallery view until you run a Signature Analysis. Once the signature analysis recognizes the file was renamed and that the file is actually an image, it displays in Gallery view.

EnCase includes built-in crash protection, which prevents corrupted graphic images from displaying in Gallery view. The timeout defaults to 12 seconds for the thread trying to read a corrupt image file. You can modify the timeout on the **Global** tab of the Options dialog.

Corrupt images tracked in the Case file so they are recognized as corrupt the next time they are accessed.

If the cache becomes full you can clear it: select the arrow dropdown menu in Evidence view and select **Clear invalid image cache**.

When viewing images in the **Gallery** tab, click a thumbnail image to see its location in the navigation trail at the bottom of the screen. To go to the location of the image, select the thumbnail and click **Go to file**.

To tag or bookmark the image, select the thumbnail and tag or bookmark as required.

Viewing Evidence

Guidance Software recommends using processed data for rapid searching and viewing of data within your case. However, there are many ways to view, filter, and find unprocessed data.

Creating Custom File Types

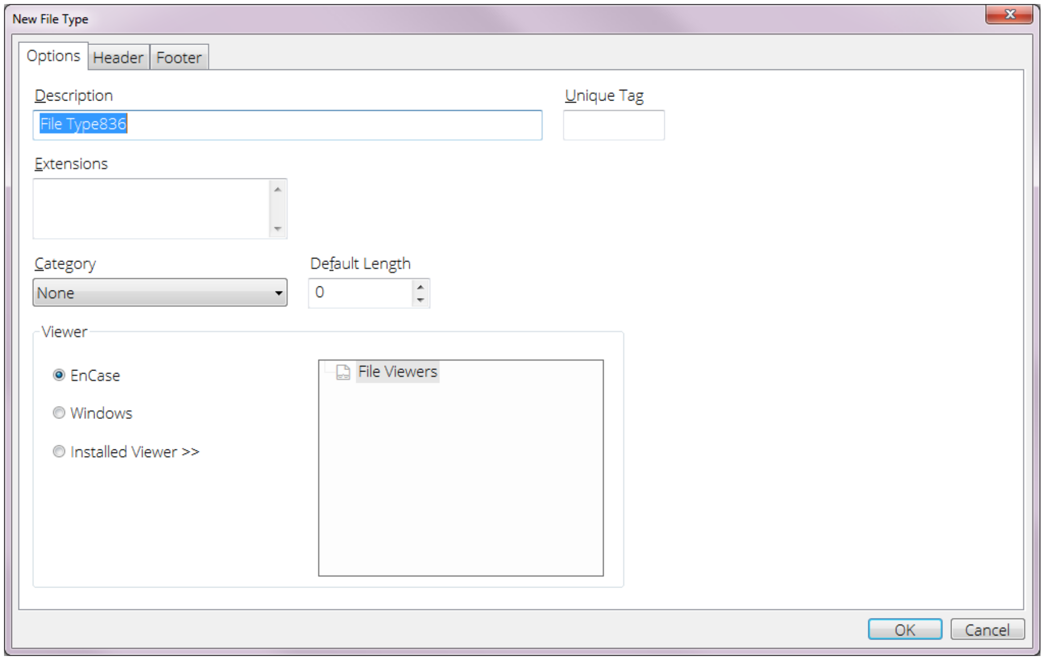
You can add your own custom file types to use with file viewers and to perform file signature analysis.

From the **File Types** tab, you can add, delete, and disable file types.

- To delete a custom file type, select it in the **File Types** tab and click **Delete**.
- You cannot delete default and shared files types.
- Checking **Disable** causes that file type to be ignored.

To add a new file type:

1. From the **View** menu, select **File Types**. The **File Types** tab displays.
2. Click **New**. The **New File Type** dialog displays.



- **Description** is the file type to associate with the file viewer.
- **Unique Tag** is a unique four character identifier that you must define for each file type.
- **Extensions** is a list of file types to associate with the file viewer.
- **Category** is the category for the type of file you are creating.
- Select a **Default Length** to determine the end of the file:
  - Use this if a footer for the file type has not been specified and is used to determine the length of the file.
  - If this is not set, a default length of 4096 bytes is used to determine the end of the file.
  - Longer lengths are recommended for pictures and ZIP files.

- The **Viewer** area contains options for selecting the type of viewer to use:
  - Click **EnCase** to associate the built-in EnCase viewer with the file type you define.
  - Click **Windows** to associate Windows with the file type you define.
  - Click **Installed Viewer** to associate an installed viewer with a file type. Use the installed viewers tree to select the specific viewer.
  - The **Installed viewers tree** lists the file viewers currently known to EnCase.

3. Use the **Header** and **Footer** tabs to specify the header and footer code defining this file type.

- The header code is the definitive identifier of the type of file. Use it when comparing against the file extension in a signature analysis.
- Use the footer code to identify the end of the file.

Viewing Multiple Evidence Files Simultaneously

1. Add the required evidence to your case.
2. View all your evidence as a list in the **Evidence** tab.
3. Select the evidence you want to expand and view as a group.
4. Click **Open**. The selected evidence displays in the **Evidence** tab.

Viewing Multiple Artifacts Simultaneously

1. In the **Artifacts** tab, select the artifacts you want to expand and view as a group, then click **Open**.
2. The selected artifacts display in the **Artifacts** tab.

The **Artifacts** tab lists all mounted volumes and results from the Evidence Processor or other activities. Therefore, Artifacts view can display multiple types of data:

- Entries (mounted archives)
- Artifacts (internet and module results)
- Email (mounted email archives)

EnCase supports viewing only one artifact type at a time. If more than one type is found in the selected artifacts, the Open Item dialog displays, enabling you to choose the artifact type you want to view. The default is **Entries**.

Note: In the Open Item dialog, only the radio buttons for the found artifact types are enabled.

Viewing Contents of 7-Zip Files

EnCase provides the ability to view the contents of 7-Zip files.

There are two ways to view 7-Zip files:

- By processing an evidence file, in which case any unencrypted 7-Zip files within are parsed automatically
- By viewing individual 7-Zip files manually

To view an individual 7-Zip file:

1. Right click the 7-Zip file you want to see. In the dropdown menu, click **Entries** > **View File Structure**.
2. EnCase parses the file and you can view its contents.

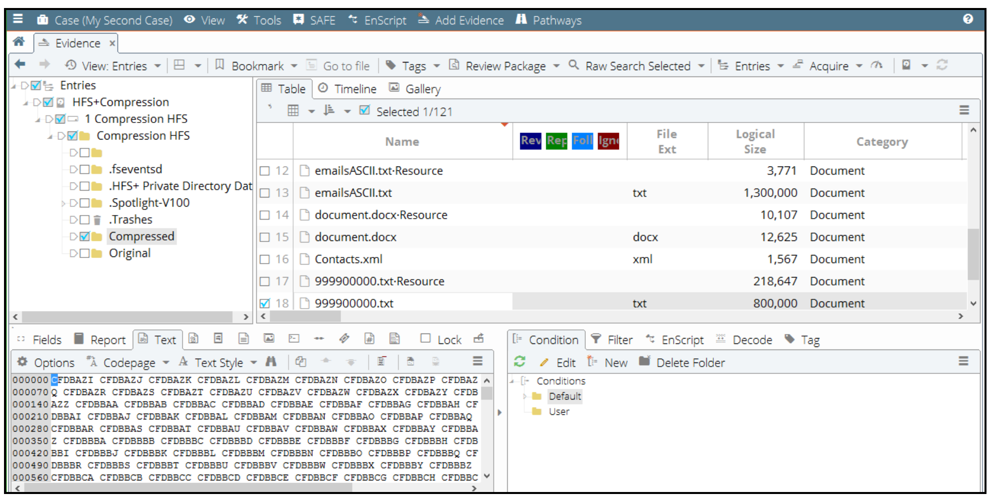
Note: If the file is protected or encrypted, a dialog displays asking for the password.

Macintosh Artifacts

EnCase Forensic supports a number of artifacts specific to the Macintosh environment.

Displaying HFS+ File System Compressed Files

EnCase displays HFS+ file system compressed files as uncompressed, and the data displays in the **Text** tab of the View pane.



Note: While loading existing evidence files that have HFS+ volumes in them, you may notice that the values for Unique Offset changed for some entries. This is expected behavior, caused by refinements in the offset computing algorithm. Unique offsets still remain unique within the given device.

HFS+ Extended Attributes

There are two types of extended attributes:

- **Internal**: The attribute size is less than 3802 bytes, and HFS+ stores the attribute inline (that is, in the same storage place as its name and size).
- **External**: The attribute size is greater than 3802 bytes, and HFS+ stores the attribute as a separate data fork

INTERNAL ATTRIBUTES

Most internal attributes are UTF-8 strings, while others are binary .plists or binary integers. EnCase attempts to convert values to strings whenever possible; if that is not possible, EnCase displays a hexadecimal representation of the data.

Extended attributes display in the **Attributes** tab of the View pane.

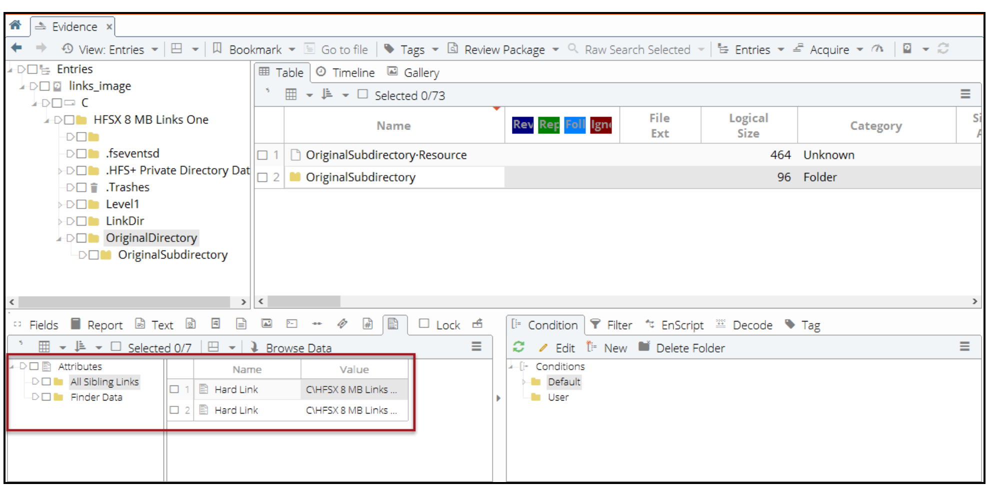
EXTERNAL ATTRIBUTES

External attributes are larger than 3802 bytes and have their own extents. For that reason, it is impractical to display them as strings. Instead, EnCase displays them as additional streams of the file they belong to. The file name is concatenated with the attribute name, separated by a middle dot (·) character.

HFS+ Directories Hard Links

Hard links for directories are specific to Mac OS X. The primary purpose is to support Time Machine, Apple's backup solution.

EnCase recognizes directory hard links and displays them with an icon that is a combination of a directory and a link. If more than one link points to the same file, these "sibling" links display in the **Attributes** tab of the View pane.



To go to the real directory a link points to, right click the link and click **Entries** > **Go to Linked File** in the dropdown menu. The directory displays in the **Fields** tab of the View pane, with the name Original Path.

Finder Data and .DS_Store

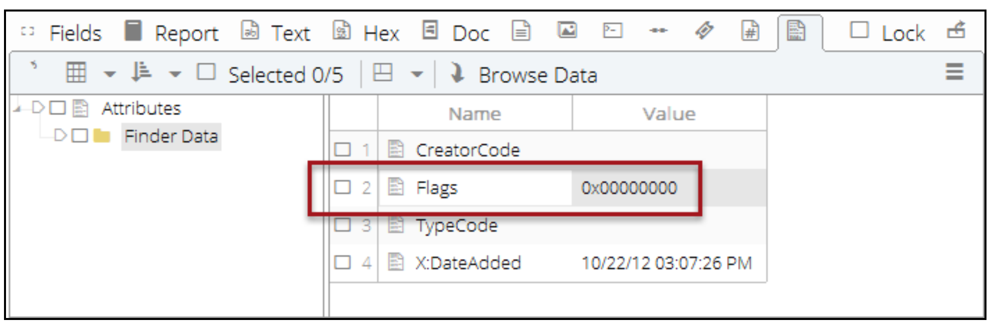
FINDER DATA

Finder data is an integral part of the HFS+ file system. This information resides in the catalog file, along with the file name, size, creation date, etc.

A Mac user can choose how information is displayed, including:

- Selecting a color for a label's background.
- Choosing to hide the file, thus preventing it from being displayed by Finder.
- Choosing to make the document a template for other documents.
- Locking the changes to the file's Finder information to prevent accidental modifications.

These are saved in the Finder Info Flags field, which EnCase decodes and displays in the **Attributes** tab of the View pane.



There are two additional fields:

- **Creator Code**, identified by OS X as `hfs+`
- **Type Code**, identified by OX S as `hlnk`

When EnCase displays Finder information, it decodes known flags and, if the background color of a file or folder was altered, EnCase also decodes the color:

.DS_STORE

The `.DS_Store` file is created inside a directory only when a Mac OS X user visits the directory using Finder. This means a directory may or may not have the `.DS_Store` file.

If a `.DS_Store` file exists, EnCase processes it on the fly when you select the **Attributes** tab in the View pane. It usually contains information about how to display items in Finder, the items' locations in the Finder window, etc.

The `.DS_Store` tags are internal and therefore undocumented, but you can deduce what some of them mean. For example, in the screenshot above:

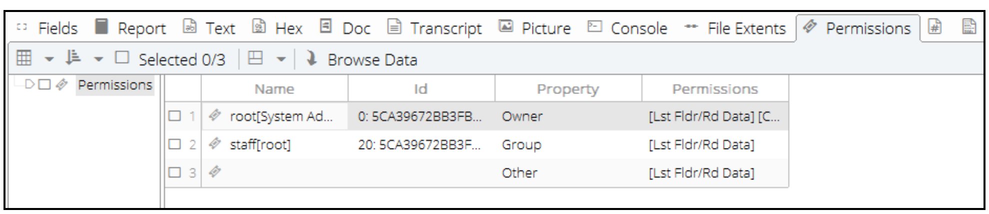
- **Iloc** is the location information, 0x263 and 0x81 being X and Y axes of the item.
- **logS** is the logical size of the item.
- **modD** and **moDD** are modification time stamps.
- **phyS** is the physical size of the item.

If you are looking for a specific tag, EnCase provides that information.

Displaying Permissions for HFS+ Files and Directories

ACCESS CONTROL LISTS

EnCase recognizes and displays Access Control Lists (ACLs), which are lists of permissions attached to an object, in the **Permissions** tab of the View pane. Here is an example of an entry with an associated Access Control List:



IMMUTABLE PERMISSIONS

EnCase displays Mac files where permission is locked as **Immutable**.

ASSOCIATING PERMISSIONS WITH TRUSTEE NAMES

EnCase displays UNIX permissions for a file or folder in the form of:

- User
- Group
- Other

If a file or folder has an Access Control List assigned to it, EnCase uses the UUID associated with users and groups, instead of the user ID or group ID.

In the image above, EnCase displays the root [System Administrator] ID as 0, the staff [root] ID as 20.

OS X DIRECTORY SERVICES

The Directory Services component of Mac OS X stores information about users and groups in a set of *.plist files, with one file per user or group. EnCase displays these in the **Table** tab of the Table pane. The paths to the file locations display in the Fields tab of the **View** pane.

VIEWING USERS AND GROUPS READ FROM AN HFS+ VOLUME

To verify that the list of users and groups is correctly populated:

1. Navigate to **View > Secure Storage**.
2. In the Table pane, click **Nix Users** or **Nix Groups**.
3. Click the hamburger menu at the far right of the Table pane, then click **User List** in the dropdown menu.
4. Depending on your selection in step 3, Nix Users or Nix Groups display in the User List dialog.

Macintosh OS X Media Containers

Macintosh OS X supports several media file formats it can mount as physical disks. These are commonly referred to as Macintosh Containers because they have their own partition schemes, file systems, and files. EnCase supports these Macintosh Containers:

- DMG
- Sparse Image
- Sparse Bundle

DMG

DMG is an Apple media file format (.dmg). Software distributed as Internet downloads use DMG as the packaging solution. Characteristics of the DMG format include:

- Single file.
- Preallocated space. Even if the DMG does not contain any data, it still has the same size as if it were full of files.
- Supports various file systems, including HFS+, and FAT. The type of file system put onto the DMG alters its format (XML metadata for HFS+, raw data for FAT). EnCase has different code paths to handle both.
- Can be encrypted via Apple FileVault.

EnCase supports these DMG formats:

- UDZO (Zip compression algorithm)
- UDBZ (BZip2 compression algorithm)
- UDCO (Apple-proprietary ADC compression algorithm)

Sparse Image

Macintosh OS X uses the Sparse Image media format to encrypt user home directories. Characteristics of the Sparse Image format include:

- Single file.
- Space is allocated by 1 MB chunks on demand, as the image data grows.
- Can be encrypted via Apple FileVault.

Sparse Bundle

Sparse Bundle is designed for efficient backups via the Apple Time Machine backup solution. Characteristics of the Sparse Bundle media format include:

- Multiple files (a directory).
- Data is contained in separate 8 MB files called "bands." The filename of each band is its number in hex.
- A file called Info.plist contains sizing information (including the size of a band and total size).
- Can be encrypted. A file called "token," which is an empty Apple FileVault file, contains all necessary information to decrypt the bands.

Here is an example of the physical directory structure of a sparse bundle container.

```
D:\Research\Mac\sparsebundle>tree /F /A sb200m.sparsebundle
D:\RESEARCH\MAC\SPARSEBUNDLE\SB200M.SPARSEBUNDLE
|   Info.bckup
|   Info.plist
|   token
|
\---bands
        0
        10
        18
        2
        c
```

Encrypting Media

All three types of media (DMG, Sparse Image, and Sparse Bundle) can be encrypted via either AES-128 or AES-256. EnCase currently supports images encrypted with AES-128 only.

Apple uses its proprietary encryption scheme, FileVault, to encrypt the media.

Adding Evidence by Dragging and Dropping Container Files to an Open Case

To add a Macintosh Container media file to EnCase as evidence:

1. Open a case.
2. Drag and drop the container (for example, a DMG file) to EnCase. EnCase displays the file in the **Evidence** tab.

EnCase supports other types of containers and encryption (if you have a valid password).

Using View File Structure with Macintosh Data

You can use the EnCase **View File Structure** function when you have acquired a Macintosh drive. You can also use it when you have a DMG or other container on a USB thumb drive add that drive as local evidence. Right click the evidence in the Name column and select **Entries** > **View File Structure** to view the contents of a container.

Viewing Processed Evidence

Processing evidence automatically indexes and performs a file signature analysis on the data. It opens compressed or compound files, including ZIP and mail archives.

The easiest way to process evidence is to run it through the Evidence Processor.

Once evidence is processed, it can be opened and viewed in ways not possible before the parsing and expanding processes are performed.

Viewing Compound Files

Compound files are compressed files or files in an embedded structure, such as ZIP files, PST email files, etc. To see all the data in a compound file, it must be run through the Evidence Processor and made into an L01 file. Compound files that are deconstructed and parsed are called "mounted" files.

To see the file structure of a compound file (manually mount), click that file and select **View File Structure**. You can also run the file through the Evidence Processor. That process creates an evidence file you can click to open or view in the **Artifacts** tab.

The following can be expanded and viewed after processing:

- Registry files
- OLE files
- Compressed files
- Lotus Notes files
- MS Exchange files
- Exchange Server Synchronization
- Outlook Express email
- Microsoft Outlook email
- Macintosh .pax files
- Windows thumbs.db files
- America Online .art files or AOL .art files
- Office 2007 docs
- ZIP and RAR archive files
- thumbs.db

Repairing and Recovering Inconsistent EDB Database Files

The Microsoft Exchange Server stores email messages in an EDB file on a server. A corresponding log file named `E##.log` stores data prior to committing it to the EDB file. When the log file contains data that has not been committed to the EDB file, the EDB file is considered to be in an inconsistent or "dirty" state. EnCase is unable to parse inconsistent EDB files.

When an EDB file is dirty, you can run several tests on it to determine whether the files are merely out of sync, or are in fact corrupt and unusable. Before running these tests, acquire the EDB database, including the entire bin and mdbdata folders. Make sure all codepages are installed on your computer.

TO RECOVER OR REPAIR A DATABASE:

The mdbdata folder contains the public and private databases and the transactional logs which are most important when cleaning a database. The BIN folder contains eseutil.exe.

1. Run `eseutil.exe` from **Windows > Start > Run**.
2. Use the eseutil.exe command line tool to check the consistency of the state field as follows:

   ```
   [file location]\eseutil /mh [filepath]priv1.edb
   [file location]\eseutil /mh [filepath]pub1.edb
   ```
3. If the EDB file is in an inconsistent state, first try to recover, as follows:

   ```
   "C:\Exchange\BIN\Eseutil.exe" /r E##.
   ```

   `/l <path>` - location of log files
   `/s <path>` - location of system files
   `/i <path>` - ignore mismatched/missing database attachments

`/d <path>` - location of database files
`/o` - suppress logo

- Note that the three-character log file base name represents the first log file.
- Files are sequentially named, with `E##.log` being the first log file.
- Click **Yes** to run the repair.

4. Run a check (step 2) on the resulting EDB file. If the file is still in an inconsistent state, attempt to repair the EDB file. This may result in the loss of some data currently in the .log files. Run the repair as follows:

```
"C:\Exchange\BIN\Eseutil.exe" /p <database name> [options]
```

`/s <file>` - set streaming file name
`/i` - bypass the database and streaming file mismatch error
`/o` - suppress logo
`/createstm` - create empty streaming file if missing
`/g` - run integrity check before repairing
`/t <database>` - set temporary database name
`/f <name>` - set prefix to use for name of report files

TO PARSE AN INCONSISTENT EDB FILE:

1. Run `eseutil.exe` from **Windows > Start > Run**.
2. EnCase checks the header of the database for its state.
3. Select the file and open **View File Structure** from the **Entries** dropdown menu.
4. The View File Structure dialog displays. If the EDB file is dirty, the dialog includes a **Scan Dirty Database** option.

   Note: If the EDB file is not dirty, the only available option is **Calculate unallocated space**.

5. To parse the dirty EDB file, check **Scan Dirty Database**, then click **OK**.

Viewing Email

You can open .PST and other types of mail storage files and view the individual emails within. You can view the higher order of email folder structure on the **Evidence** tab. Once the email is processed, you can double click the storage file to drill down to the individual mail messages.

The default view for Email is the Tree view. This shows the report in full screen, in as close to native format as possible. Empty fields do not display in the report view. The **Fields** tab shows all available metadata about the email and its collection, including the Transport Msg ID.

Use the **Search Results** tab and **Find Email** to view data across multiple repositories. You may also want to view all your indexed evidence and then show only items with an item type of Email. You can further drill down by finding subsets of sender, date range, etc.

EnCase allows you to track email threads and view related messages. Before you can analyze email threading, you must have already run the Evidence Processor against your case evidence with the **Find email** option selected. To avoid displaying the same message multiple times, EnCase removes duplicate messages in both the Show Conversation and Show Related email views.

To view an email message:

1. In the **Artifacts** tab, double click the .PST file whose emails you want to search. The archive displays in a new expanded tab.
2. Select an email to view in the View pane.

Viewing Attachments

In the tree view, email attachments display as children under the parent email.

EnCase allows you to view attachments on email messages that you select.

To view the content of an attachment:

1. In the **Evidence** tab, select the message with the attachment that you want to view.
2. Click the **Doc** button in the View pane. EnCase displays the contents of the message attachment.

Showing Conversations

Email threading is based on conversation-thread related information found in the email message headers. EnCase uses email header metadata (including message ID and in-reply-to headers) to reconstruct email conversation threads. Email conversation thread reconstruction is done during processing, so conversations are not available on data that has not been processed.

Different email systems use different methods of identifying conversations. For example:

- The header fields *Message-ID*, *Reply-To-ID*, and *References*.
- The header field *Conversation Index*.
- The header field *Thread-Index*.
- *Multiple mechanisms*, because the messages of interest cross email system boundaries. In these cases, EnCase builds a separate conversation tree for each type of data found in the header (for example, one using *Message-ID/References* and another using *Conversation Indexes*) and displays the conversation tree containing the most email.

EnCase can display conversations for all supported email types except AOL, because AOL messages do not store thread-related information. However, the feature cannot always reconstruct complete conversations when the conversations include messages from multiple email systems. For example, EnCase cannot fully recreate a conversation where some users are using Outlook, some are using Lotus Notes, and others Thunderbird.

If an email does not have any of the message header fields specified above, EnCase cannot construct a conversation thread for it. Selecting such an email and clicking **Show Conversation** results in a tree containing only the selected email.

Before you can analyze email threading, you must have already run the Evidence Processor against your case evidence with the **Find email** option selected.

To show an email conversation:

1. In the **Evidence** tab select an email or email store in the Table pane.
2. From the **Find Related** menu, select **Show Conversation**.

Displaying Related Messages

All email messages with identical subject lines are considered related and displayed together. Viewing related messages can sometimes produce more comprehensive results than browsing through conversation threads.

EnCase can show related emails for all supported email types. Since Show Related only looks at the subject line of a message, the emails displayed may not all be related, depending upon the uniqueness of the subject line.

To show related messages:

1. In the **Evidence** tab select an email or email store in the Table pane.
2. From the **Find Related** menu, select Show Related Messages.

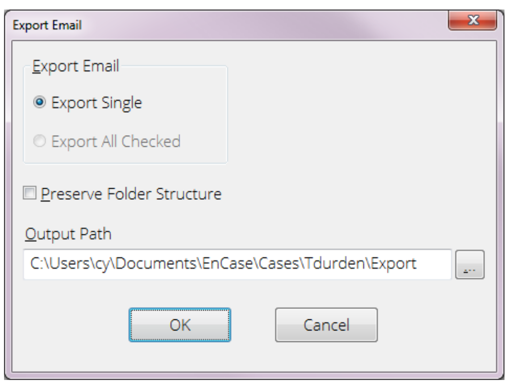
Showing Duplicate Email Messages in a Conversation

By default, when you view an email conversation, EnCase hides any duplicate email messages in that conversation. To show all duplicates in a conversation, click **Show Duplicates** in the **Show Conversation** or **Show Related** view toolbar. Duplicate email messages display with red alerts that indicate their status.

Exporting to *.msg

The Export to .msg option for mail files and mail file attachments lets you preserve the folder structure from the parsed volume down to the entry or entries selected. This option is available for the highlighted entry or selected items.

1. In the Tree pane, select the email message(s) you want to export.
2. Right click and select **Export to *.msg**. The Export Email dialog displays.



   - **Export Single** exports only the selected message.
   - **Export All Checked** exports all files checked.
   - **Preserve Folder Structure** saves selected email folder structure information.
   - **Output Path** captures the location of the export data file. The default is `[username]\Documents\EnCase\Cases\[Case name]\Export`.

3. Click **OK**. View the folder structure in the Export folder. Double click a message to view it in read-only format.

CHAPTER 8

SEARCHING THROUGH EVIDENCE

Overview	245
Searching Indexed Data	246
Finding Tagged Items	257
Keyword Searching Through Raw Data	257
Refreshing Search Results during a Keyword Search	260
Retrieving Keyword Search Results	261
Bookmarking Keyword Search Results	262
Analyzing Individual Search Results	262
Viewing Saved Search Results	262
Creating a LEF from Search Results	264
Finding Data Using Signature Analysis	264
Exporting Data for Additional Analysis	268
Exporting Search Results for Review	272

Overview

EnCase Forensic provides three principal methods of searching through evidence:

- Index searches
- Tag searches
- Keyword searches through raw data

You can use these search methods by opening the **Indexed Items**, **Keyword Hits**, and **Tagged Items** tabs from either the **Home** page of the case or from the **View** menu.

Index Searches

Index searching allows you to rapidly search for terms in a generated index, and is the recommended search method in EnCase Forensic. Querying an index for your case or evidence file locates terms much more quickly than using non-indexed queries. Unlike raw keyword searches, indexing is linked with file transcript content so that text content contained with files can be quickly and efficiently identified. You can also conduct metadata and field searches to locate content with greater precision.

EnCase Forensic indexes evidence using a modified version of Lucene index and search technology. You can search through the index using standard Lucene query syntax and most Lucene search operators and term modifiers.

Indexes are generated using the Evidence Processor. An index can encompass all evidence in your case.

- See Creating an Index on page 148 for information about creating and running index searches.
- See Searching Indexed Data on the next page for a full list of search syntax options.

> **Note:** Index search is a two step process. First, you index data using the Evidence Processor. In the second step, you retrieve indexed data by executing a search in the **Indexed Items** tab.

Tag Searches

EnCase also provides the capability to search for items that have been flagged with user-defined tags. Using tags, you can search through collected evidence for all items that include one or many tags. See Finding Tagged Items on page 257 for information about creating and running tag searches.

Note: Tagged searches are a two step process. First, you tag the data to be searched. In the second step, you retrieve tagged data by executing a search in the **Tagged Items** tab.

Keyword Searches through Raw Data

You can query the results of a previously executed keyword search. You create keyword searches either with the Evidence Processor or by performing a raw search on your case data. Keyword searching searches the raw binary form of a file. It does not search the metadata of the file.

- See Retrieving Keyword Search Results on page 261 to view the results of a previously executed keyword search.
- See Adding a New Keyword on page 145 to learn how to add a new keyword from the Evidence Processor or when performing a raw search.
- See Creating a New Keyword List on page 147 to learn how to add a new keyword list.

Note: Keyword searches are a two step process. First, you perform a keyword search on raw data. In the second step, you retrieve keyword data by executing a search in the **Keyword Hits** tab.

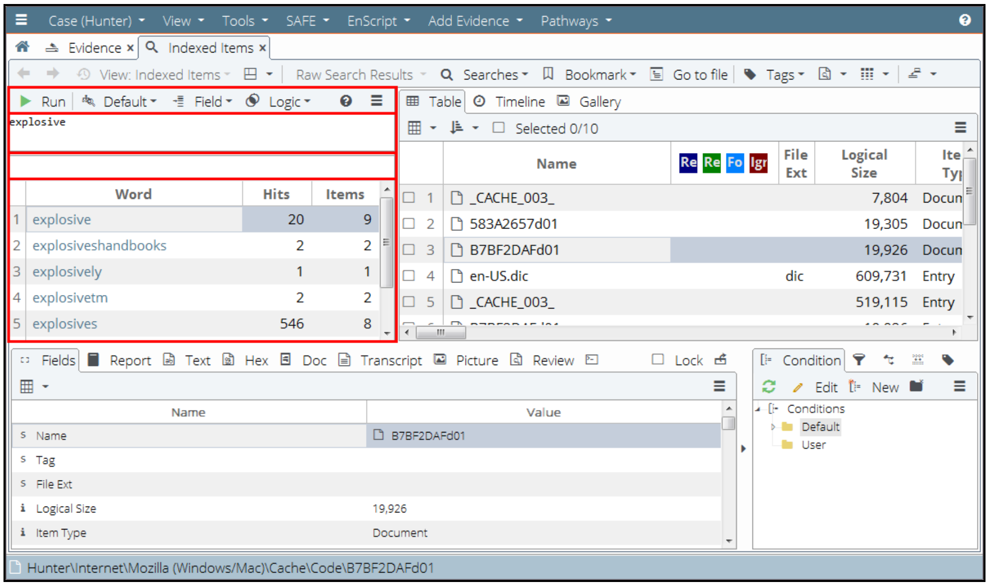
Viewing and Saving Search Results

Any set of search results can be saved and viewed later. See Viewing Saved Search Results on page 262 for details.

Searching Indexed Data

Searching through indexed data is the quickest way to find a specific subset of evidence items. To perform an index search, you must have selected the Index Text and Metadata option prior to evidence processing. See Creating an Index on page 148 for more information on indexing.

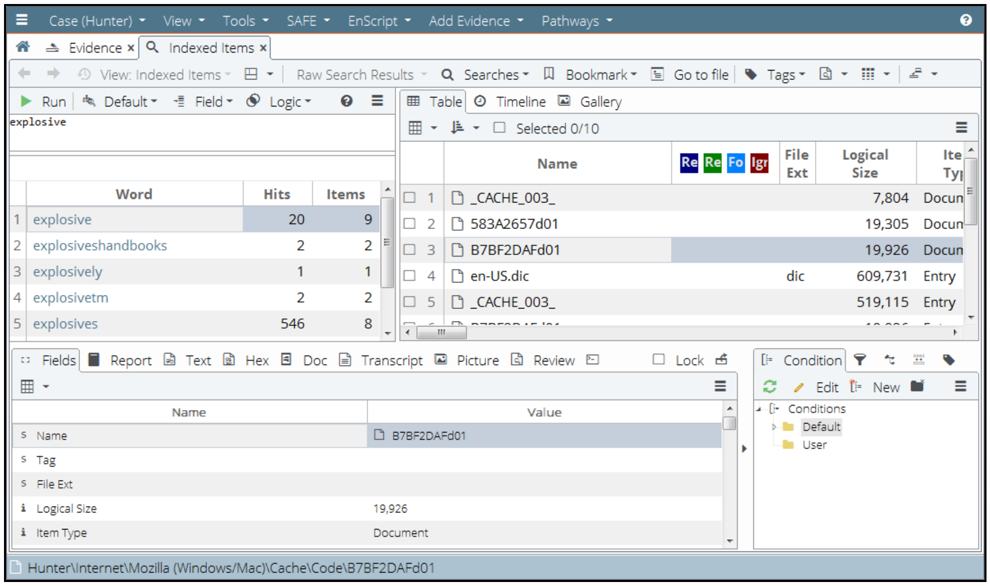
Search through indexed data in the Indexed Items tab. The Indexed Items tab is divided into four standard panes. The upper left pane is the query pane:



- **Query Actions Bar**: Provides options to run a query entered in the Query Construction Box, change the default language index, select a field to search, add a Boolean operator, access online help, or access other options.
- **Query Construction Box**: Type or paste a query directly into the box below the Query Action Bar. This box is used to create more complex queries.
- **Quick Query Box**: For a quick index search, enter a single word directly into the box below the Query Construction Box.
- The **Quick Query Results Table** is found below the Quick Query Box and displays search results of quick query words, number of hits, and number of items that contain the query word. Related words are also displayed with hit and item count.
- **Table Pane**: When a query is executed, all items that contain the queried items display in the table pane on the right.
- **View Pane**: Details of the item selected in the table pane can be viewed here.

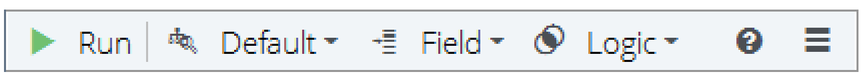
To search indexed data:

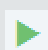
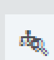
1. Open the **Indexed Items** tab from either the **Home** page of the case or from the **View** menu.



2. Type your search query in the Query Construction Box, paste a query, or select available query options from the Query Actions Bar.

   The query actions bar provides tools for constructing a search query. Expand the left pane to view all buttons and drop-down options. Right click the mouse in the query window to view these commands in the context menu.



Icon	Name	Description
	Run	Run the current query and view results.
	Default/Multiple	Select the language index to search. The dropdown menu lists all languages selected during evidence processing. Default is optimized for English and can be used with most Western languages. To search the index of another language, check the box from the dropdown menu.

Icon	Name	Description
	Field	Opens a dropdown menu where you can target a specific data field for your search. After adding the field name, enter the value you want to find in the Query Construction Box.
	Logic	Inserts a Boolean `AND`, `OR`, `+`, `NOT`, or `–` operator into the Query Construction Box. Operators must be capitalized.
	Help	Open online help for searching indexed data.
	Options Menu	Access additional options: • **Print** opens a dialog to print the query or export to PDF. • **Export** exports to a file. • **Line Numbers** enables you to display or hide line numbers in the query box.

- **Ctrl+Enter** adds a line to the Query Construction Box.
- View a list of search syntax options at Search Operators and Term Modifiers below.

3. To run the search query in the Query Construction Box, position your cursor in the text box and click **Enter**, or click the **Run** button.

The Quick Query Box and Quick Query Results box automatically display the most recent search term entered in the Query Construction Box. You can enter a term in the Query Construction Box or Quick Query Box to instantly show all variations of the occurrence of that term. Click a hyperlinked term in the Word column to show all occurrences of that term in the right table pane.

Search Operators and Term Modifiers

EnCase Forensic indexes evidence using an implementation of Lucene index and search technology. You can search the index using standard Lucene query syntax, and most Lucene search operators and term modifiers. Search operators and term modifiers from Lucene are summarized below. For more information on Lucene search operators and term modifiers, see

the Apache Lucene project at https://lucene.apache.org/core/6_4_2/queryparser/org/apache/lucene/queryparser/classic/package-summary.html#package.description.

Boolean Operators

Boolean operators allow for the combination of terms through the use of logical operators. Boolean operators must be formatted in ALL CAPS. The following operators are supported:

OR

The `OR` operator is the default conjunction operator and is used when no other operator is specified. The `OR` operator links two terms and finds matching documents if either term is found in the document. The term `||` may also be used interchangeably with the `OR` operator.

`George OR Washington` returns documents containing "George" or "Washington"

AND

The `AND` operator matches documents where both terms are present anywhere in the text of a single document. The term `&&` may also be used interchangeably with the `AND` operator.

A search for `"George Washington" AND "Washington George"` return documents that contain the terms, "George Washington" and "Washington George".

+

Use the `+` operator to make the term following it required. The term after the `+` operator must exist in a document for it to be returned in a search.

A search for `+Washington George` returns documents that must contain the term "Washington" and may contain "George".

NOT

The `NOT` operator excludes documents that contain the term after the NOT operator. The term `!` may also be used interchangeably with the `NOT` operator.

> **Note:** The NOT operator must include at least one non-excluded search term. Submitting a search with only a NOT operator returns no results. For example, the search `NOT "George Washington"` returns no results.

-

The – operator excludes documents containing the term after the – symbol.

`"George Washington" -"Washington George"` returns all instances of "George Washington" but excludes documents with instances "Washington George"

Terms and Phrases

EnCase Forensic supports two search terms types: single terms and phrases. Single terms are single words. Phrases are a group of words enclosed in quotes.

Search terms are highlighted in the search results. Phrase searches highlight the individual terms of the phrase as well as the whole phrase.

Perform an exact phrase search by enclosing the phrase in quotes.

`"George Washington Carver"` searches for the exact phrase, "George Washington Carver"

With Two Variables

Use parentheses to group multiple words within a search term. For example, in this search term:

```
"Bill (Clinton OR Gates)"~5
```

the index marks as responsive all items containing the word Bill within five words of either Clinton or Gates.

With Multiple Variables

You can also construct a complex proximity search that includes Boolean operators on both sides. For example, in this search expression:

```
"(Bill AND William) (Clinton AND Gates)"~5
```

the index marks as responsive all items containing both the words "Bill" and "William" within five words of both "Clinton" and "Gates."

Grouping

Use parentheses to group clauses and control the Boolean logic of a query. How you use parentheses determines the search order. Subqueries are performed first. For instance:

```
(George AND Washington) OR (Abraham AND Lincoln)
```

finds all items with either both the terms "George" and "Washington" or both the terms "Abraham" and "Lincoln."

You can nest parenthetical expressions. For example:

```
(George AND (Washington OR Bush))
```

finds all items containing the term "George" and either the terms "Washington" or "Bush."

Alternatively:

```
(George AND Washington) OR Carver)
```

finds all items containing both the terms "George" and "Washington", or the term "Carver".

You can join proximity queries (`~x`) to Boolean logic queries (`AND`, `OR`). For example:

```
Delaware AND "George Washington"~3
```

finds all items containing the term "Delaware" that also contain the terms "George" up to three words from "Washington."

FIELD GROUPING

You can use parentheses to group multiple single terms or phrases. For example:

```
from:(Carver AND "George Washington")
```

returns documents where the `from` field contains both the search term "Carver" and the phrase "George Washington."

Range Searches

Range searches locate matches where field values fall between the lower and upper bounds specified in a range query. A range query with square brackets is inclusive. A range query with curly brackets is exclusive.

```
logical_size:[500000 to 1000000]
subject:{allen TO zebra}
```

Date Searches

Search for items by date range using field syntax:

```
last_accessed:[20170101 TO 20170102]
```

Search for a time range by appending the time in six-digit format to the bounding dates:

```
file_created:[20170101080000 TO 20170101130000]
```

The above term searches for any item with a creation date between January 01, 2017 08:00 and January 01, 2017 13:00, including the bounding times and dates.

Using Wildcards to Search for Patterns

Search for incomplete words using the `?` and `*` operators. Wildcards are supported within single words, but not within phrase queries.

WILDCARD FOR SINGLE CHARACTERS

The `?` operator stands as a placeholder for any single character. For instance, a search for:

```
c?t
```

results in hits in documents containing cat, cot, and cut, but not caught.

WILDCARD FOR MULTIPLE CHARACTERS

The `*` operator stands as a placeholder for any number of characters. For instance:

```
ind*
```

results in hits for documents containing indecisive, indignant, and Indiana.

The [*] operator can also be used within a word. For instance:

```
in*ive
```

results in hits for documents containing indecisive, initiative, and intuitive.

MULTIPLE WILDCARDS

A term can contain multiple wildcards (either `*` or `?`), but cannot contain wildcards as the first character of the term. For instance:

```
ind*a*a
c?t?
p*fi?y
```

are valid searches terms. However:

```
*india*
?cat?
*fis?
```

are not valid search terms.

Regular Expression Searches

The forward slash / marks the beginning and end of a regular expression. The indexing engine searches for patterns that match the regular expression contained within the slashes.

Format

```
/regular expression/
```

Example

`/[jb]ump/` finds all documents containing the words "jump" and "bump"

Proximity

The tilde ~ acts as a proximity operator when it follows a phrase containing two terms. Perform a proximity search on two terms by enclosing the terms in quotes, appending the tilde ~ and adding a numeric value. The numeric value represents the maximum number of words that can exist between the two search terms for a positive hit to be returned. While proximity search can return results where the second search term appears before the first search term, the proximity value must be increased by two in order to account for counting through the first word and locating the beginning of the second word.

Format

```
"searchterm1 searchterm2"~<value>
```

Example

`"George Washington"~3` finds all documents where the word "Washington" appears three words or less after the word "George" or where the word "Washington" appears immediately before the word, "George"
`"white house"~10` finds all documents where the word "house" appears ten words or less after the word "white" or where the word "house" appears eight words or less before the word, "white"

Fuzzy Searches

The tilde ~ acts as a fuzzy search operator when it follows a single search term. The fuzzy search operator returns results similar to the term. Append an optional integer from 0 to 2 to specify the search tolerance. If no number is specified, a default value of 2 is used. The larger the number, the broader the search.

Format

```
searchterm~
searchterm~<value>
```

Example

`file~` returns similar terms like "mile", "pile" and "files"

Search Fields

EnCase Forensic searches for terms in every indexed text field. You can restrict the fields you search using the field name followed by a colon `:`. For example, to search for terms in the subject line, use:

```
subject:George
```

You can use parentheses to group terms together in a field:

```
subject:(George AND Washington)
```

You can perform field searches with other search functions:

```
subject:"George Washington"~2
```

To search in a specific Item Type, choose Item Type from the Field drop-down, and select category you want to search. Search options include: None, Entry, File, Email, Document, and Record. When you make a selection, the item type and corresponding number for the category are entered in the query box. Enter the AND operator, followed by your query, and click the Run button to conduct the Item Type search.

```
item_type:3 AND "George Washington"
```

Search Fields

The following table lists supported fields.

Individual Fields		
Action URL	From	Received
BCC	Icon Data	Requesting URL
CC	Icon URL	Sent
Comment	Item Path	Subject
Description	Item Type (None, Entry, File, Email, Document, Record)	Symbolic Link
Entropy	Last Accessed	To
Entry Modified	Last Written	True Path
Entry Slack	Logical Size	URL Host Name
File Created	Metadata	URL Name
File Ext	Name	Unique Offset
Pattern Fields		
Credit Card (<p:CreditCard>)	Phone Number (<p:CreditCard>)	Social Security Number (<p:SocialSecurityNumber>)
Email Address (<p:EmailAddress>)		

Reserved Characters

EnCase Forensic supports escaping special characters that are used in query syntax. The following characters must be escaped if you want to use them as part of a search:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```

The Escape Character (\)

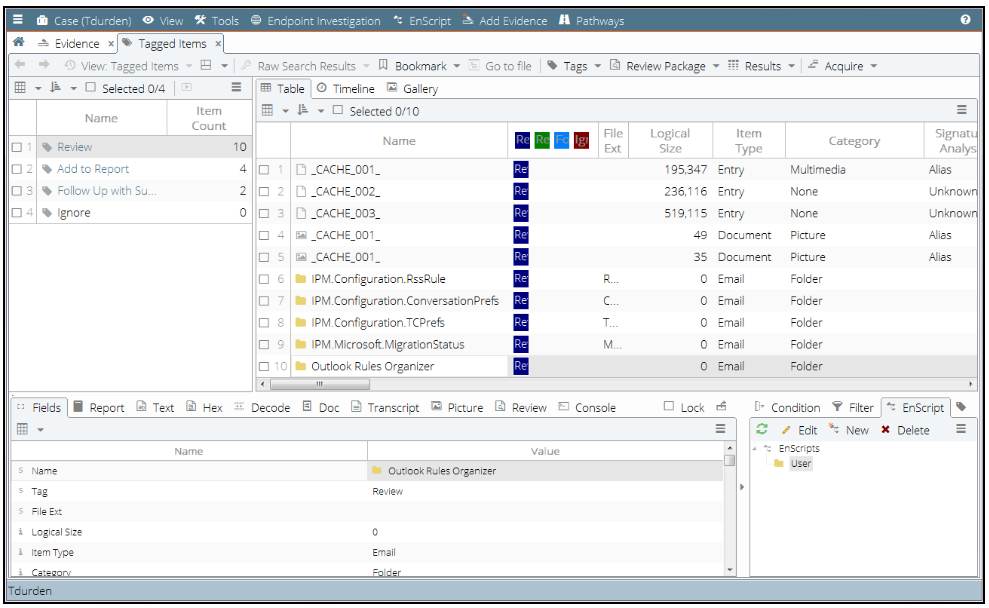
The escape character (\ ) defines an escape sequence, transforming special characters and words into their literal versions.

For example, to search for `(3-2=1):1`, use the escape character before each special character: `\(3\-2=\)\:1`

Finding Tagged Items

Finding tagged data enables you to quickly review items that have been flagged for special attention. Clicking in the tag column in the table pane automatically adds or removes a tag from that item.

1. Open the **Tagged Items** tab from either the **Home** page of the case or from the **View** menu.



2. Click on a tag directly to display all items with that tag in the table pane.
3. Select multiple tags and click **View Selected** to see items containing any of the selected tags.

Keyword Searching Through Raw Data

Although index searching is the recommended type of search, there may be times when you want to perform a search across the raw contents of a device. In those cases, you can perform a keyword search on your non-indexed case data. Keyword searching only searches the raw binary form of a file, so some content may not be discovered if it is compressed or otherwise hidden.

SEARCHING REMOTE DEVICES

You can perform hashing and raw keyword searches on remote devices.

In order to maximize performance, you can search and hash these types of files remotely:

- Uncompressed, unencrypted and/or non-resident files
- NTFS compressed files
- EFS encrypted files
- Resident files

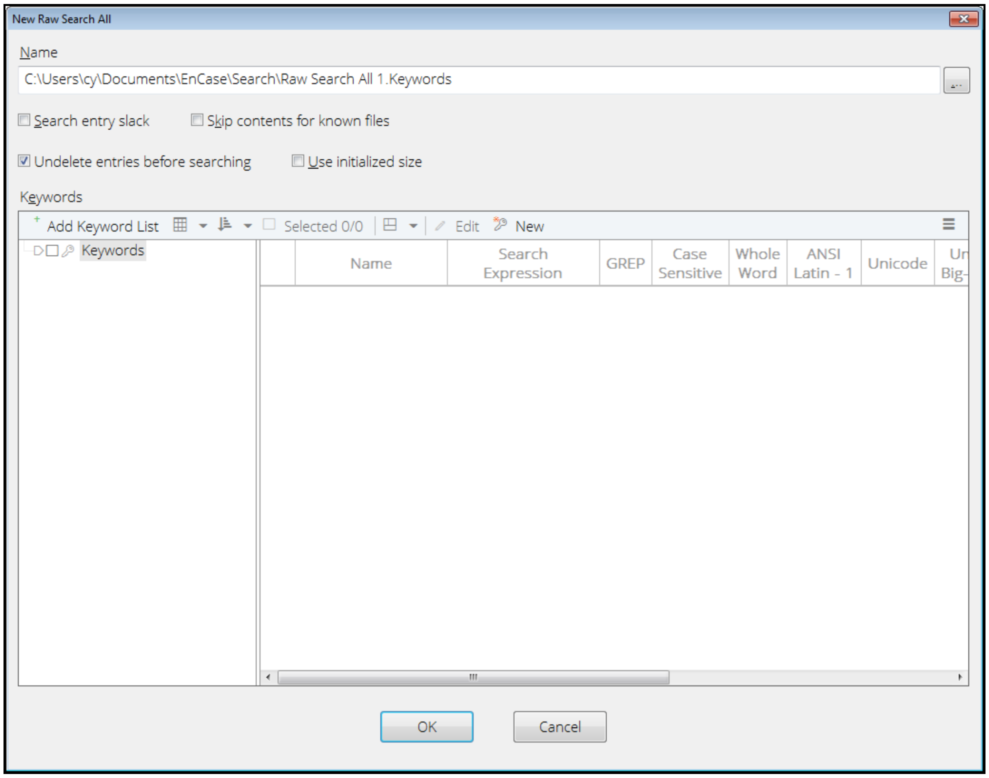
You cannot search and hash encrypted files (other than EFS) remotely.

To create a new raw keyword search within a case:

1. In the **Evidence** tab, select the device(s) to search.

   Note: You can also create a new raw keyword search for specifically selected items by going to the **Entry** > **Raw Search Selected** menu.

2. Click **Raw Search All**.
3. Select an existing search or click **New Raw Search All** to create a new search. The New Raw Search All Entries dialog displays.



- Use the path box at the top of the dialog to specify the name and location for the search.
- Select **Search entry slack** to include file slack in the keyword search.
- Select **Skip contents for known files** to search only the slack areas of known files identified by a hash library.
- Select **Undelete entries before searching** to undelete deleted files before they are searched for keywords.
- **Use initialized size** lets you search a file as the operating system displays it, rather than searching its full logical size.
  - In NTFS and exFAT file systems, applications are allowed to reserve disk space for future operations. The application sets the logical size of the file larger than currently necessary to allow for expected future expansion, while setting the Initialized Size smaller so that it only needs to parse a smaller amount of data. This enables the file to load faster.
  - If a file has an initialized size less than the logical size, the OS shows the data area between the initialized size and logical size as zeros. In actuality, this area of the file may contain remnants of previous files, similar to file slack. By default, EnCase displays, searches and exports the area past the initialized size

- as it appears on the disk, not as the OS displays it. This lets you find file remnants in this area.
  - Select Initialized Size to see a file as its application sees it and the OS displays it.
  - Note that when a file is hashed in EnCase, the initialized size is used. This means that the entire logical file is hashed, but the area past the initialized size is set to zeros. Since this is how a normal application sees the file, this lets users verify file hashes with another utility that reads the file via the OS.

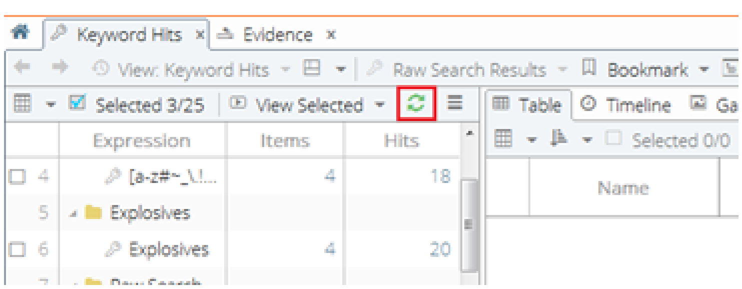
- **Add Keyword List** opens a dialog where you can enter a list of words and assign certain properties to them as a group. See Creating a New Keyword List on page 147.
- **Split Mode** lets you configure the layout of the dialog.
- **New** opens the New Keyword dialog where you can add a new keyword. See Adding a New Keyword on page 145.
- Double click a keyword, or click **Edit**, to open the keyword and modify its properties.
- Highlight a keyword and click **Delete** to remove it from the list.

4. When you finish, click **OK** to save the search.

Refreshing Search Results during a Keyword Search

When running a raw keyword search, you can view the search hits while the search is ongoing, instead of waiting for the entire search to complete.

To see search results while the search is in progress, click the **Refresh** icon on the **Keyword Hits** tab.



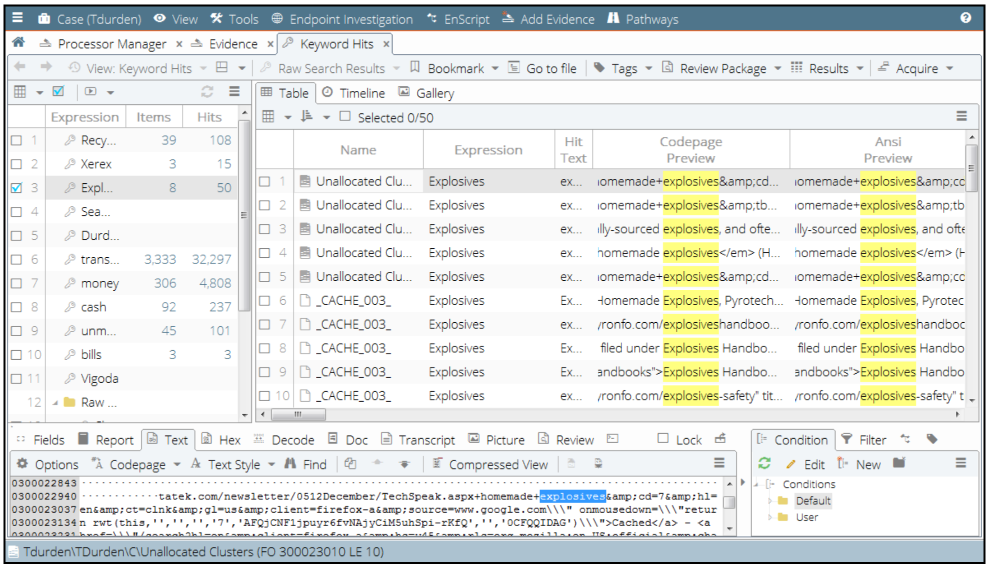
If new search hits are available, the icon displays in green. If no new search hits are available, the icon is disabled.

The icon is dynamic: after clicking, it is disabled until more search hits are available. When more search hits are available, the icon is enabled and displays again in green.

Retrieving Keyword Search Results

You can retrieve previously executed keyword search results from the **Keyword Hits** tab.

1. Open the **Keyword Hits** tab from either the **Home** page of the case or from the **View** menu.
2. A list of keywords displays. These are the keywords that have been previously executed.



3. View keyword results by items or hits.
   - Click an Items column hyperlink to see all responsive items for that keyword in the Table pane.
   - Click a Hits column hyperlink to see all responsive hits for that keyword in the Table pane.

4. Select multiple keywords and click the **View Selected** button to see a combination of all search results.
5. Choose **View Items** or **View Hits** from the **View Selected** dropdown to view keyword results by items or hits.

Bookmarking Keyword Search Results

You can create keyword hit bookmarks from the **Keyword Hits** tab. Right click the keyword hit and click **Bookmark > Keyword Hit**. You can also bookmark multiple selected keyword hits at one time. Right click the keyword hit and click **Bookmark > Selected Keyword Hits**.

Analyzing Individual Search Results

Use the viewing options at the bottom of the **Indexed Items, Keyword Hits, Tagged Items** or **Results** tabs to see information about a single search result in a variety of ways.

- Use the **Review** tab to see a compressed list of metadata, keyword item, and index search hits.
  - This tab combines information found on the **Fields**, **Transcript**, and **Text** tabs, showing fields and individual lines containing search hits.
  - Click the linked Search Hits line number to view the search hit on that line in context.
  - Use the **Next/Previous Item** buttons to click through each item in the list.

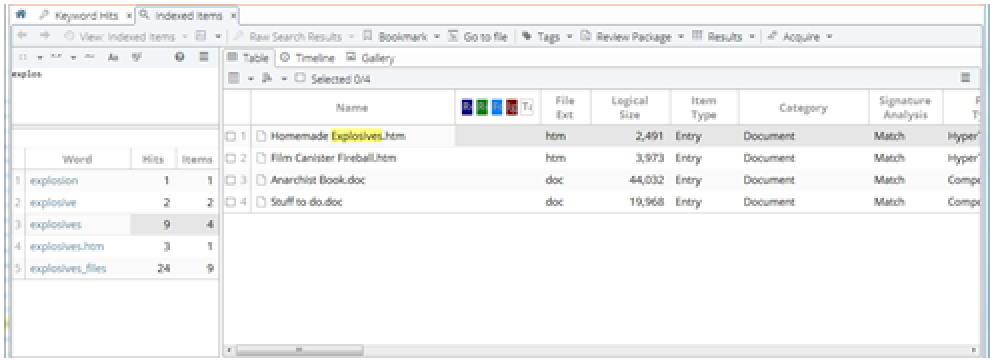
- Content hits are also highlighted in the **Transcript**, **Text**, and **Hex** tabs while metadata hits are highlighted in the **Fields** tab.
  - Click **Compressed View** on the **Transcript**, **Text**, and **Hex** tabs to see only the lines containing highlighted search hits.
  - Use the **Next/Previous Hit** buttons to click through each hit in the file. If there are no more hits in the file, the next item opens and the first hit is found.

For more information about viewing options, see Viewing Content in the View Pane on page 202.

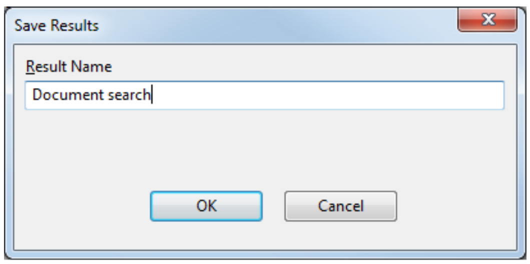
> **Note:** Index hits with large numbers of characters that wrap over line breaks do not display in the **Review** tab.

Viewing Saved Search Results

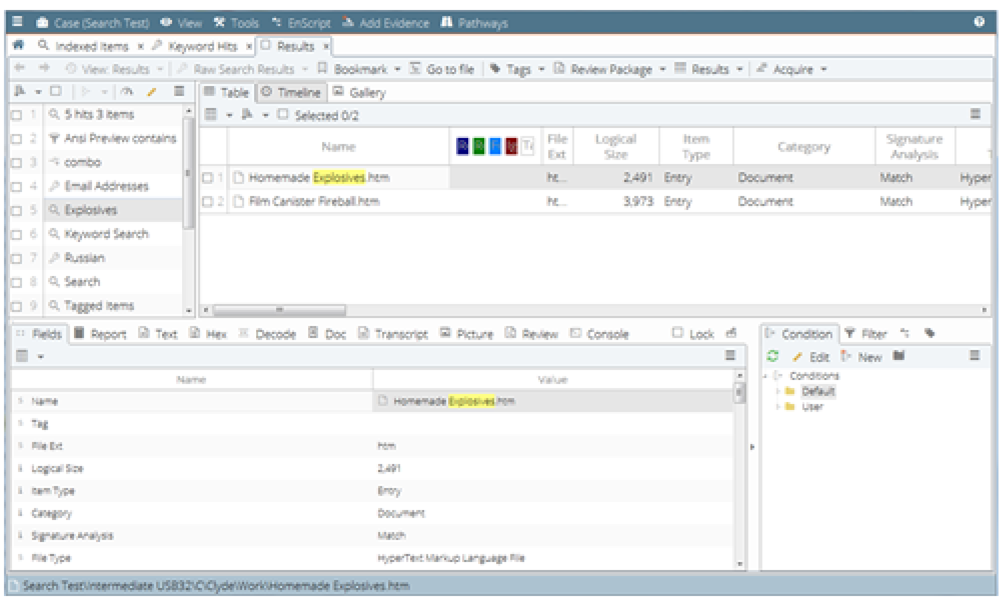
1. Collect a set of search results and click the Results toolbar button. Then click **Save Results**.



2. The Save Results dialog displays.



3. Enter the name for your search and click **OK**.
4. From the **View** menu, select **Results**. The **Results** tab displays.



5. Select a saved search in the left pane. The results of that search display in the right Table pane. Click individual items to see more information in the lower viewing tabs.

Note: If you save search results when viewing by hits in the **Keyword Hits** tab, only unique items are saved. For example, if you select ten hits that occur in one item and three that occur in another, only the two unique items will be saved in the result set. You can create keyword hit bookmarks if you wish to save individual keyword hits. See Retrieving Keyword Search Results on page 1

Creating a LEF from Search Results

You can export items in a set of search results to a LEF. Search results can contain both entries and artifacts.

When you export search results containing only entries or containing only artifacts, EnCase generates a single LEF.

When you export search results containing both entries and artifacts, EnCase generates two LEFs, one containing only artifacts and another containing only entries.

1. On the **Indexed Items**, **Keyword Hits**, or **Tagged Items** tab, select the items you want to export.
2. Click **Acquire** > **Create Logical Evidence File**.
3. EnCase exports the items you checked to a LEF.

Note: If you choose both entries and artifact items, the records are exported to a LEF named `<UserCreatedName>.artifacts.L01`.

Finding Data Using Signature Analysis

Signature analysis compares file headers with file extensions in order to verify file type. For standardized file types, a signature, or recognizable file header, is always associated with a specific file type extension.

File extensions are characters following the dot in a file name (for example, signature.doc). They often indicate the file's data type. For example, a .txt extension denotes a text file, while .doc indicates a document file.

The file headers of each unique file type contain identifying information called a signature. For example, .BMP graphic files have **BM** as a signature.

A technique often used to hide data is to attempt to disguise the true nature of the file by renaming it and changing its extension. Because a .jpg image file assigned a .dll extension is not usually recognized as a picture, comparing a file’s signature with its extension identifies files that were deliberately changed. For example, a file with a .dll extension and a .jpg signature should pique the interest of an investigator.

The software performs the signature analysis function in the background on all processed evidence.

Information about results of a file signature analysis displays in Evidence tables, in the Signature Analysis column:

- **Match** indicates data in the file header, extension, and File Signature table all match.
- **Alias** means the header is in the File Signature table but the file extension is incorrect (for example, a JPG file with a .ttf extension). This indicates a file with a renamed extension. The word Alias displays in the Signature Analysis column, and the type of file identified by the file signature displays in the File Type column.
- **Unknown** means neither the header nor the file extension is in the File Signature table.
- **!Bad Signature** means the file's extension has a header signature listed in the File Signature table, but the file header found in the case does not match the File Signature table for that extension.

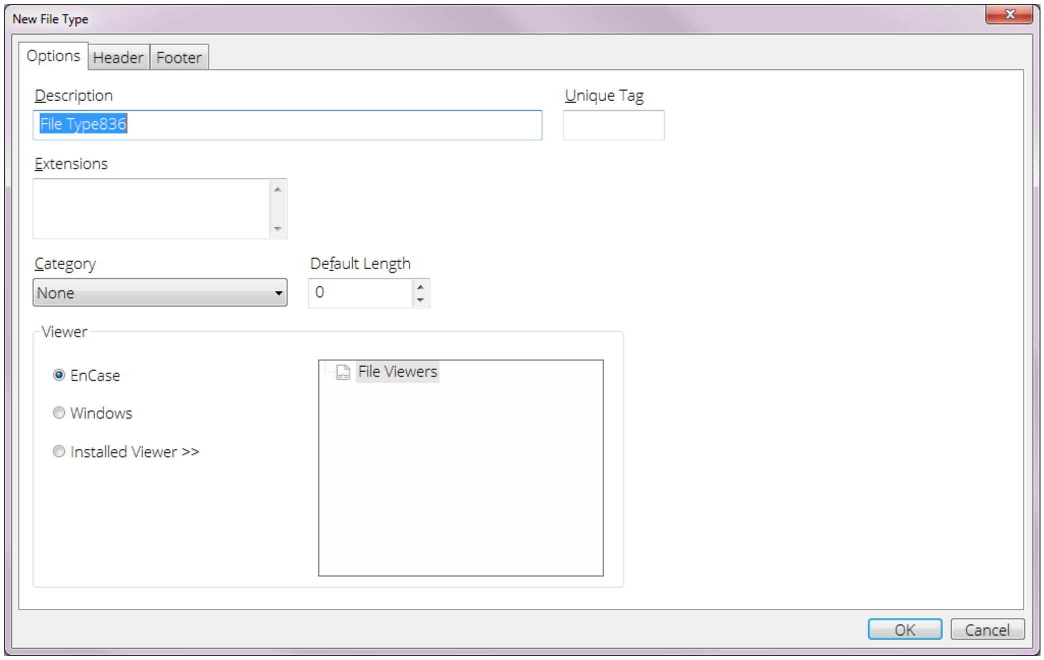
Adding and Modifying File Signature Associations

All file signatures are associated with file types in the File Type table.

Occasionally a file signature may not be in the table. Use this procedure to add a new one. Before you do this, you need to know the file signature search expression. This is not necessarily the same as the three letter file extension.

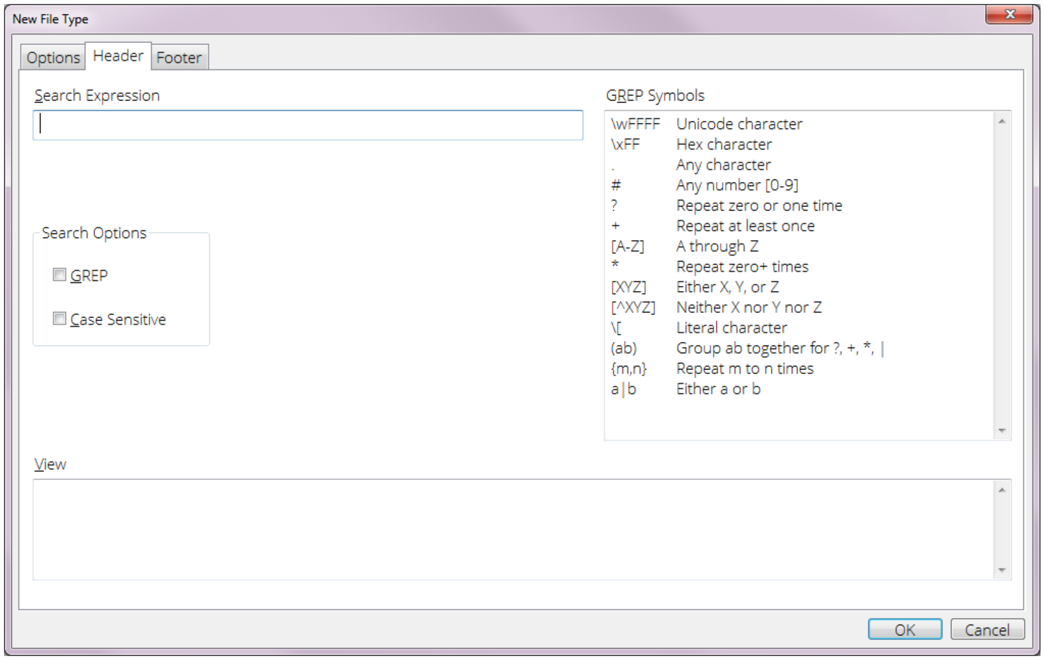
To add a new file signature and file type:

1. From the **View** menu, select **File Types**. The File Type table displays.
2. Click **New**. The New File Type dialog displays.



- Create a descriptive name for the new file type.
- Enter one or more three letter extensions for the file type, on separate lines of the Extensions text box.

3. Click the **Header** tab to display the file signature information.



- Enter the file signature in the Search Expression field.
- Select **GREP** if the expression uses GREP variables to locate the file signature.
- Select **Case Sensitive** if case sensitivity is desired.

4. Click **OK**. The new file type and associated file signature are added to the table.

To change an existing file signature:

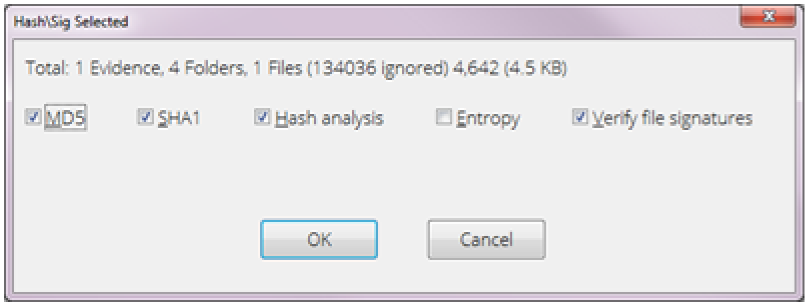
1. From the **View** menu, select **File Types**. The File Type table displays.
2. Double click a file type. The Edit File Type dialog displays.
3. Click the **Header** tab to display the file signature information.
4. Change the **Search Expression** and other options as desired, then click **OK**.

Note: If you modify a built-in file type, it is marked as User Defined. EnCase does not overwrite User Defined file types, even when you install a new version of EnCase.

Running File Signature Analysis against Selected Files

Using the Evidence Processor, you can run file signature analysis on a previewed device without first acquiring the device.

1. On the **Evidence** tab, drill into the device where you want to run file signature analysis.
2. Blue check the specific files you want to run signature analysis on.
3. Click **Entries**. In the dropdown menu, click **Hash\Sig Selected**. The Hash\Sig Selected dialog displays.



- **MD5** generates MD5 hash values for the selected files.
- **SHA1** generates SHA1 hash values for the selected files.
- **Hash analysis** compares the hash values of selected files against hashes in your library.
- **Entropy** creates entropy values for the selected files.
- **Verify file signatures** performs file signature analysis on the selected files.

4. Select **Verify file signatures** to run signature analysis. You can also select other processes to run concurrently.
5. Click **OK**.

Note: After running file signature analysis, you must refresh the device. Click the Refresh button in the Entries toolbar.

Exporting Data for Additional Analysis

You can copy files in their native format from EnCase to other media or folders for sharing or further analysis. This feature can also recover and restore deleted files on a byte-per-byte basis.

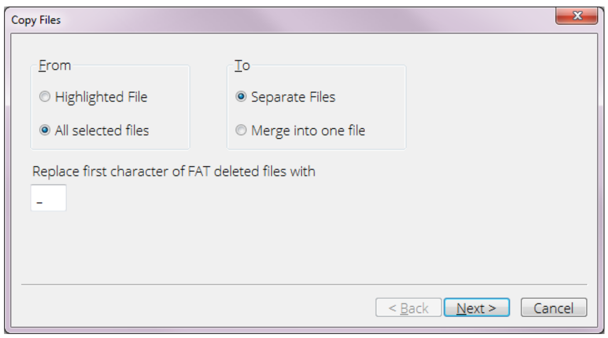
You can copy both files and folders. Copying folders preserves their internal structure.

EnCase allows you to automatically navigate to the directory where your files are saved. Click the **Open Destination Folder** checkbox on the Destination dialog to launch Windows File Explorer with the export location.

Copying Files

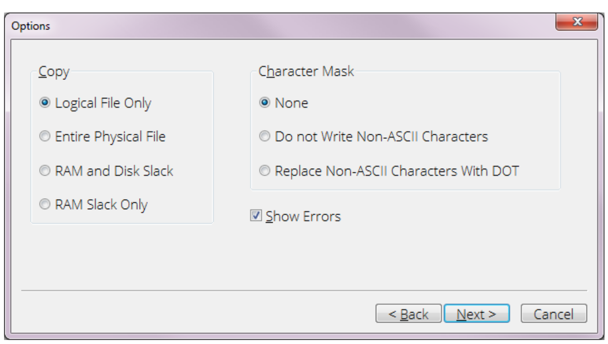
To copy files:

1. In the **Evidence** or **Artifacts** tab, click the **Entries** dropdown menu and select **Copy Files**.
2. In the **Results**, **Indexed Items**, **Keyword Hits**, or **Tagged Items** tab, click the **Results** drop-down menu and select **Copy Files**.
3. The Copy Files dialog displays.



- Select **Highlighted File** to copy the highlighted file.
- Select **All selected files** to copy the currently selected files in the table.
- **Separate Files** outputs each file to its own file.
- **Merge into one file** merges the output of all selected files into one file.
- **Replace first character of FAT deleted files with** determines which character is used to replace the first character in the filename of deleted files in the FAT file sys-tem. Deleted files on a FAT volume have a hex \xE5 character at the beginning. The underscore (_) character is used by default to replace this character.

4. Click **Next**. The Options dialog displays.



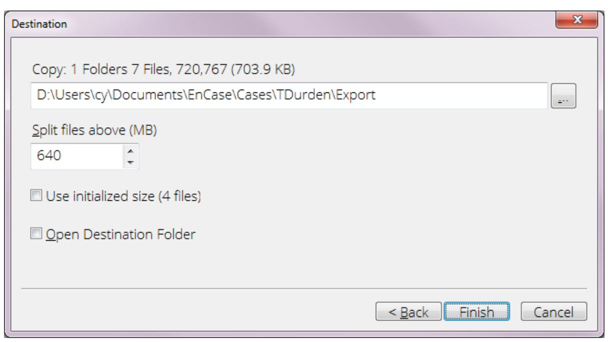
- **Copy Files** contains settings that determine the content of the evidence file to be copied.

- Logical File Only performs the copy function on the logical file only, not including the file slack.
- Entire Physical File performs the copy function on the entire physical file, including the logical file and file slack.
- RAM and Disk Slack performs the copy function on both the RAM and disk slack.
- RAM Slack Only performs the copy function on the RAM slack only.

- The Character Mask settings determine what characters are written into the file or files created by the copy function.
  - Select None if you do not want any characters masked or omitted from the filenames of the resulting files.
  - Select Do not Write Non-ASCII Characters to mask or omit non-ASCII characters from the filenames of the resulting files. All characters except non-ASCII characters are retained.
  - Select Replace NON-ASCII Characters with DOT to replace non-ASCII characters with periods in the filenames of the resulting files.

- Checking Show Errors causes the application to notify you when errors occur. This prevents the unattended execution of the Copy Files operation.

5. Click Next. The Destination dialog displays.



- Copy displays the number of files to be copied, and the total number of bytes of the file or files created.
- Path shows the path and filename of the file or files to be created. The default is `My Documents\EnCase\[case name]\Export`.
- Split files above contains the maximum length, not exceeding 2000MB, of any file created by the Copy Files function. When the total number of bytes in an output file exceeds this value, the additional output continues in a new file.

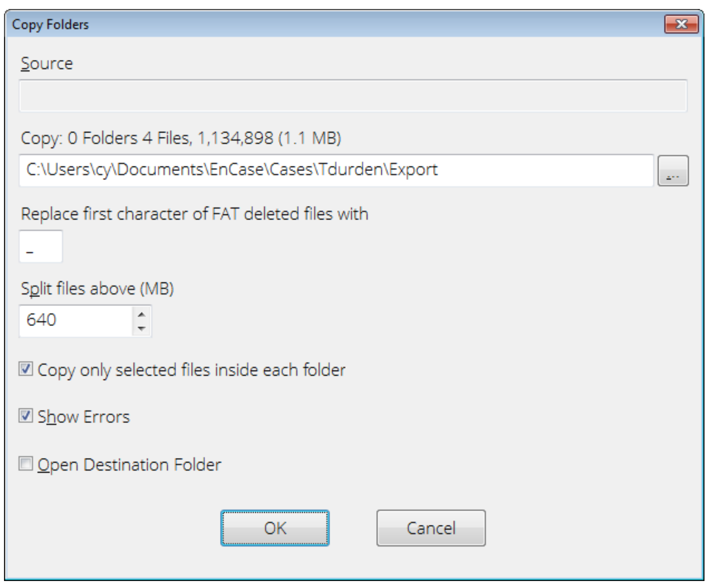
- **Use Initialized Size** determines whether to use the initialized size of an entry, rather than the default logical size or the physical size. This setting is only enabled for NTFS and exFAT file systems. When an NTFS or exFAT file is written, the initialized size can be smaller than the logical size, in which case the space after the initialized size is zeroed out.

6. Click **Finish**. The Copy Files operation executes. The resulting files are saved in the directory specified in the Destination dialog.

Copying Folders

1. Select the folder or folders to copy.
2. Open the Copy Folders dialog:
   - In the **Evidence** or **Artifacts** tab, click the **Entries** dropdown menu and select **Copy Folders**.
   - In the **Results**, **Indexed Items**, **Keyword Hits**, or **Tagged Items** tab, click the **Results** dropdown menu and select **Copy Folders**.

3. The Copy Folders dialog displays.



Select the desired options:

- **Source** displays the folder to copy.
- **Copy** displays the number of files to copy, and the total number of bytes in the file or files created.

- **Path** shows the path and filename of the file or files to be created. The default is `My Documents\EnCase\[case name]\Export`.
- **Replace first character of FAT deleted files with** determines which character is used to replace the first character in the filename of deleted files in the FAT file system.
- **Split files above** contains the maximum length, not exceeding 2000 MB, of any file created by Copy Folders. When the total number of bytes in an output file exceeds this value, the additional output is continued in a new file.
- **Copy only selected files inside each folder** copies individual files selected within a folder or folders.
- Checking **Show Errors** causes the application to notify you when errors occur. This prevents the unattended execution of the copy operation.
- **Open Destination Folder** opens the selected folder when the copy action completes.

4. Click **OK**.

Exporting Search Results for Review

You can consolidate search results into a review package that can be reviewed by external parties. Review packages can be a combination of email or file results from indexed or raw keyword searches. You can also create review packages from bookmarks. The review package is a self-contained application viewable in a web browser that does not require EnCase in order to open and work with it. Reviewers can use existing tags or make customized tags for flagging items of interest in the review package. When the information is imported back into EnCase, using a generated .EnReview file, you can then see the tags added by the reviewer.

All file types can be packaged for review. Raw and indexed searches cull through the content and metadata of pictures, email, and office documents. Metadata information is culled for other file types.

The process for creating, reviewing, and returning a review package follows this work flow:

- The EnCase examiner searches and compiles a results list that is exported into a review package.
- The reviewer receives and opens the review package.
- The reviewer browses through and analyzes the contents of the review package. Existing tags can be used or the reviewer can create customized tags.

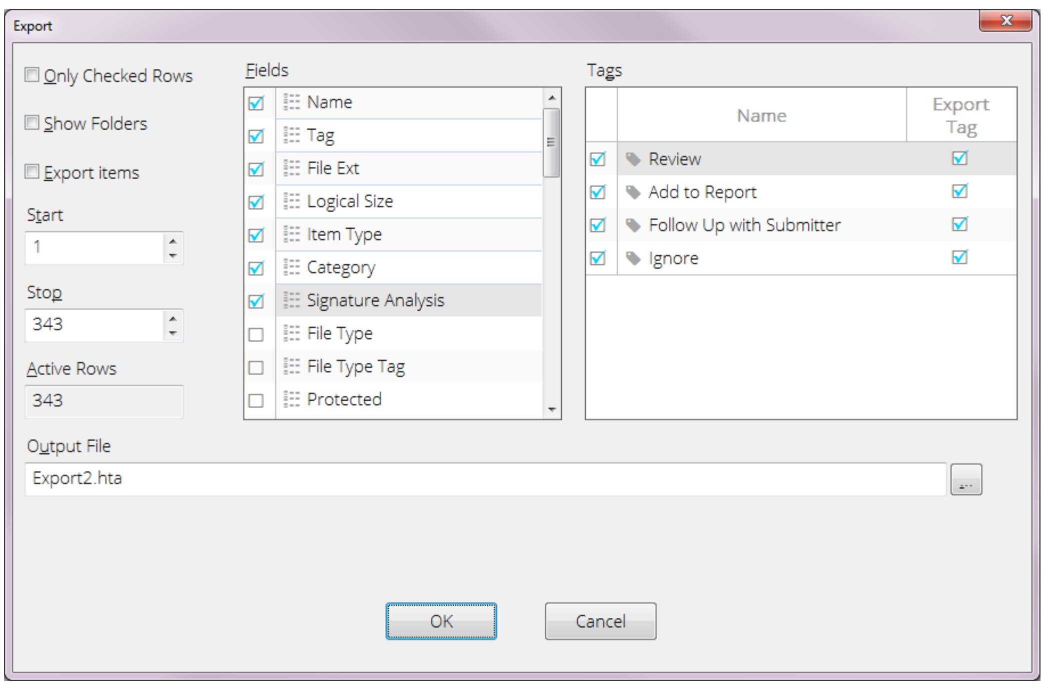
- The reviewer exports the tagged review package and sends the exported file back to the EnCase examiner. The export package contains only the GUIDs of the items, so it can be emailed back as a small file without revealing any case information.
- The EnCase examiner imports the analyzed review package and views the tagged items in EnCase.

Creating a Review Package

After you perform a search, you can package a set of results for external review. Both email artifacts and files can be reviewed.

To create a review package:

1. From any item view, select **Review Package** > **Export**.
2. The Export dialog displays. Select the appropriate options to create the review package:



   - **Only Checked Rows** exports the selected rows in the current table view of the search list. If a range of rows is selected, only checked rows within that range are exported. When cleared, all rows in the current table view are exported.
   - **Show Folders** exports items along with any relevant folder structure. When selected, all items are exported. When cleared, only items in the current table view are exported. You must select this option when exporting selected items from multiple folders to the review file.

- **Export Items** exports files in their native formats as part of the review package. EnCase exports all file types except raw File System entries (for example: $MFT, $LogFile or any '$*' files on NTFS file systems). Unallocated Clusters and Unused Disk Area are not exported.

When you open the review web browser, the Review Export function displays hyperlinks which, when selected, open the associated original files.

- Select the fields you want to export in the **Fields** list.
- By default, all tags are automatically exported for use by the reviewer. Clear the checkboxes on the left for any tags you do not want to export.
- The **Export Tag** checkbox determines whether to export the tagging information already entered on any of the items. When cleared, any tagging choices you made are omitted from the review package. When checked, your tagging selections remain intact.
- Enter or browse to the name and path for the export files.

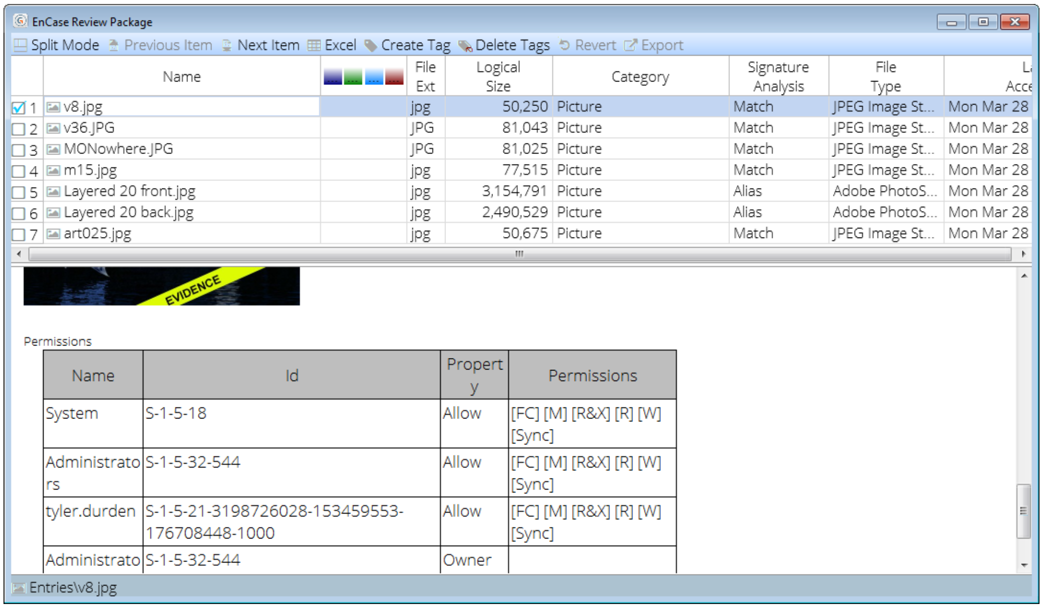
3. Click **OK**. A status bar displays the export process. When the export process completes, the review package window opens to allow the examiner to confirm its contents. Include the ReviewPackage.hta and the accompanying \ReviewPackage.data folder when compiling the Review Package for distribution.

Analyzing and Tagging a Review Package

Review Packages are created much like web pages. They have an .hta extension and can be opened by Windows as a native .html application.

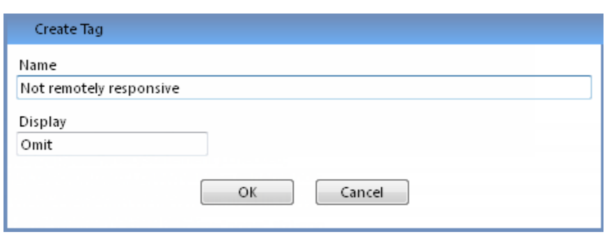
The review application displays two panes. The upper pane displays the items exported from EnCase. The lower pane displays specific information about the currently selected item.

1. To open an .hta review package, double click the .hta file. The EnCase Document Review window displays.



2. Scroll through the items on top and use the lower pane to review their content.
3. Click the area of the tag column beneath the desired tag to tag or untag an item.
   - You can expand the tagging column to see the names of tags.
   - You can tag each item with as many tags as desired. Newly added item tags display a plus icon.
   - Click an existing item tag to delete it. A minus icon displays where the item tag was before.
   - Item tags added by the original examiner are included in the review package. Item tags specified by the original examiner can be removed.
   - When reviewing bookmarks, each bookmark displays on a separate row so separate tags can be applied to individual bookmarks. These bookmarks are aggregated within the item when reviewed in EnCase.

4. To create a customized tag, click **Create Tag** in the menu bar. The Create Tag dialog displays.



   - Enter the name for the tag in the Name text box.
   - If you want to display a shorter name, enter it in the Display text box.
   - Click **OK** to create the tag and close the dialog.

5. To delete one or more tags, click **Delete Tags** in the menu bar. The Delete Tag dialog displays.
   - Check the tag(s) you want to delete.
   - Click **OK** to delete the tags and close the dialog.

6. Tags can always be reverted to their last saved state. The last saved state is the state the tags were in when they were originally imported, or the state they were in the last time the review package was exported with the **Commit Changes** checkbox checked.

   To revert to the last saved tagging choices, click **Revert** in the menu bar. The Revert dialog displays.

   - Check each tag you want restored to its last saved state.
   - Click **OK** to revert the tags and close the dialog.

Exporting a Review Package

You can create an .EnReview file from a review package to send to an EnCase examiner to import. When generating an .EnReview file, only the GUID and tag information of the items are captured, so there is no case information included in the file. The export file is small enough to be sent through email. Only changes from the last saved state are stored in the export file.

1. To export a review package to be imported into EnCase, click **Export** in the menu bar. The Export dialog displays.
   - Check **Commit Changes** to save the current set of tags.
     - Committing changes updates the review package's last saved state.
     - The last saved state is then used as a baseline for future modifications.

   - Enter the path for the review package to be saved.

2. Click **OK**. The review package is exported and saved as an .EnReview file in the desired location.
3. Send the .EnReview file to the EnCase examiner to import back into EnCase.

   Note: When a case is exported via Review Package, the HTA file displays a maximum of 31 tags.

Importing a Review Package

1. To import reviewed data select **Review Package** > **Import** from the toolbar. The Import dialog displays.

2. Enter the path where the .EnReview file is stored and click **Next**. A list of tags added to the review package displays.
    - Only tags with changes since the last saved change display in the list.
    - Clear checkboxes for any tags you do not want to import.
    - Item tags present when the review package was exported, then subsequently removed by the reviewer, are removed in the examiner's case when you import the returned review package.
    - If multiple reviewers are analyzing the same review package, the same rules apply to each .EnReview file.
        - If an item tag was present when the review package was exported, and one reviewer removed it while another reviewer left if in, then the tag is removed in the examiner's case when you import the returned review packages.
        - The order in which you import the review packages does not make a difference.

3. When you are done, click **Finish**. The tag changes in the review package are incorporated into EnCase.

    Note: Tags applied to separate bookmarks within a particular item are aggregated; therefore, each item in EnCase displays all tags that were applied to all its bookmarks.

CHAPTER 9

HASHING EVIDENCE

Overview	281
Hashing Features	281
Working with Hash Libraries	282
Integration with Project VIC	292

Overview

Analyzing a large set of files by identifying and matching the unique hash value of each file is an important part of the computer forensics process. Using the hash library feature of EnCase, you can import or custom build a library of hash sets, allowing you to identify file matches in the examined evidence.

A hash function is a way of creating a digital fingerprint from data. The function substitutes or transposes data to create a hash value. Hash analysis compares case file hash values with known, stored hash values.

The hash value is commonly represented as binary data written in hexadecimal notation. If a hash value is calculated for a piece of data, and one bit of that data changes, a hash function with strong mixing property will produce a completely different hash value.

Hashing creates a digital fingerprint of a file. A fundamental property of all hash functions is that if two hashes (calculated using the same algorithm) are different, then the two inputs are different in some way. On the other hand, matching hash values strongly suggests the equality of the two inputs.

Computer forensics analysts often create different hash sets of known illicit images, hacker tools, or non-compliant software to quickly isolate known "bad" files in evidence. Hash sets can also be created to identify files whose contents are known to be of no interest, such as operating system files and commonly used applications. Hash sets are distributed and shared among users and agencies in multiple formats. These formats include NSRL, EnCase hash sets, Bit9, and others.

Until recently, the MD5 hash calculation was the hash set standard to identify a file. Large hash distribution sets, such as the NSRL set, are now distributed using the SHA-1 hash calculation. EnCase uses an extensible format for hash sets that allows:

- Storing metadata along with the hash value in field form.
- Support of MD5, SHA-1, and additional hash formats within the same file structure.
- Storing tags associated with items in the hash set.

Hashing Features

EnCase hashing features include the following:

- A versatile user interface for hash library management that allows:
    - Creation of hash sets and libraries.
    - Importing and exporting hash sets.
    - Querying hash sets.
    - Viewing hash sets or individual hash items.

- Hash libraries that can contain multiple hash sets. Each set can be enabled or disabled.
- Ability to create as many hash libraries or hash sets as needed.
- Ability to report every match, if a hash belongs to multiple hash sets in a library.
- Ability for each case to use a maximum of two different hash libraries at the same time.

Note: When using the 32-bit Examiner to edit a large number of hash sets, you may see an error message stating "Not enough storage is available to process this command." This is a limitation of the 32-bit Examiner. Guidance Software recommends you use the 64-bit Examiner.

Working with Hash Libraries

A hash library is a folder containing a database-like structure where EnCase stores hash sets. To work with hash libraries, click **Tools** > **Manage Hash Library**. The Manage Hash Library dialog displays.

You can use this dialog to:

- Create a new hash library or open an existing library.
- Create new hash sets in a library or edit an existing hash set in a library.
- Import and export hash sets from one library to another.
- Associate hash sets with hash libraries and hash libraries with cases.
- Query a hash library for a particular value.
- Manage hash items, including viewing and deleting hash items.

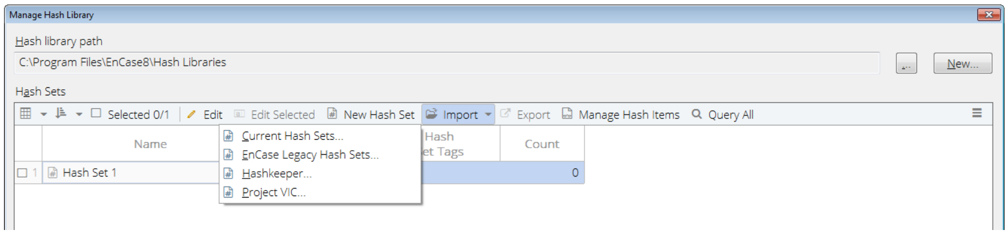
Creating a Hash Library

To create a hash library:

1. Click **Tools** > **Manage Hash Library**.
2. In the Manage Hash Library dialog, click the **New** button in the upper right corner.
3. Browse for a folder to hold the hash library. If you use an existing folder, it must be empty; otherwise, the contents of the folder will be deleted.
4. Click **OK**.
5. The path and name of your hash library now display in the hash library path field.

To import hash sets from another library into an existing hash library:

1. Click **Tools** > **Manage Hash Library**. The Manage Hash Library dialog displays.



2. Click **Import** from the toolbar, and select an option:
   - Current Hash Sets
   - EnCase Legacy Hash Sets
   - Hashkeeper
   - Project VIC

3. A path dialog opens. Locate and select the hash set.
4. Click **Finish**.

You can then browse to a library or enter Hashkeeper identification data to import individual hash sets. To create new hash sets for this library, see Creating a Hash Set below.

Creating a Hash Set

Hash sets are collections of hash values, representing unique files, usually belonging to a common group. For example, a hash set of all Windows operating system files could be created and named Windows System Files. When you run a hash analysis on an evidence file, the software identifies all files included in that hash set. You can then exclude those logical files from later searches and examinations. This speeds up keyword searches and other analytic functions.

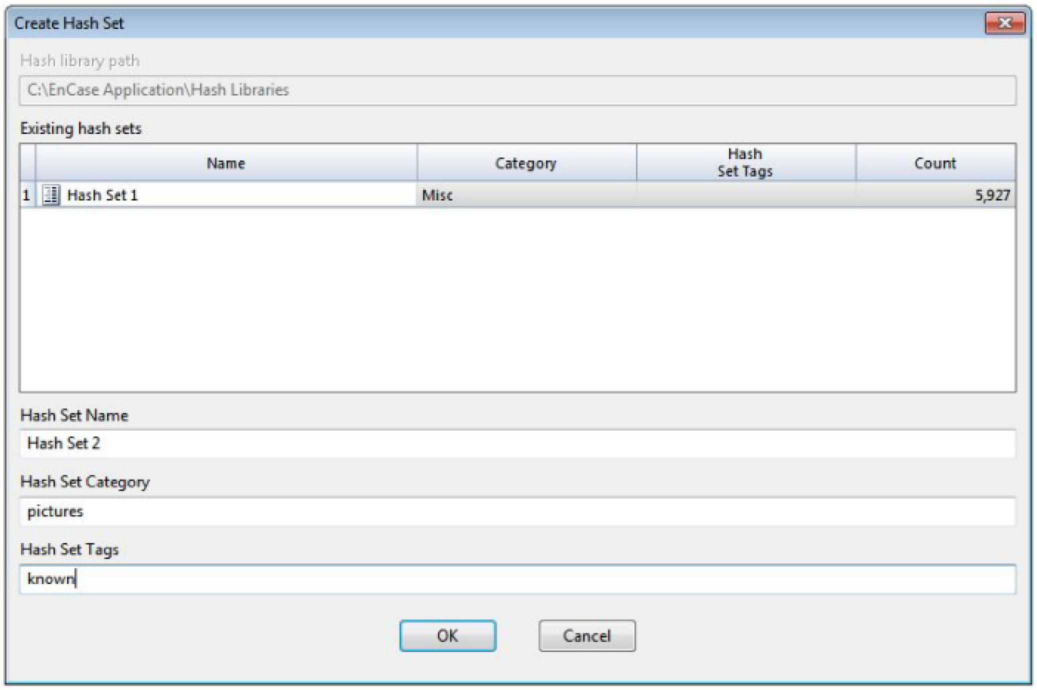
Once created, you can add to hash sets on a case by case basis. Adding new files as time goes by saves time and effort in subsequent investigations.

Hash sets (which contain individual hash entries) are located within hash libraries. Creating a hash set is a two step process. The first step is to create an empty hash set in a library. The second step is to add information to it.

To create a hash set:

1. Click **Tools** > **Manage Hash Library**.
2. Make sure that you either browse and point to an existing hash library or create a new one. This is the hash library where you will add the hash set.

3. In the Manage Hash Library dialog, click **New Hash Set**. The Create Hash Set dialog displays



4. Enter a **Hash Set Name**, and enter information for **Hash Set Category** and **Hash Set Tags**.
    - You can use the hash set category to identify the type of hash set. Although the most common values are Known and Notable, you can specify any single value. You can use the category to find or eliminate files.
    - Hash set tags allow you to specify multiple identifiers for a hash set. As with hash set categories, you can use hash set tags to find or eliminate files.

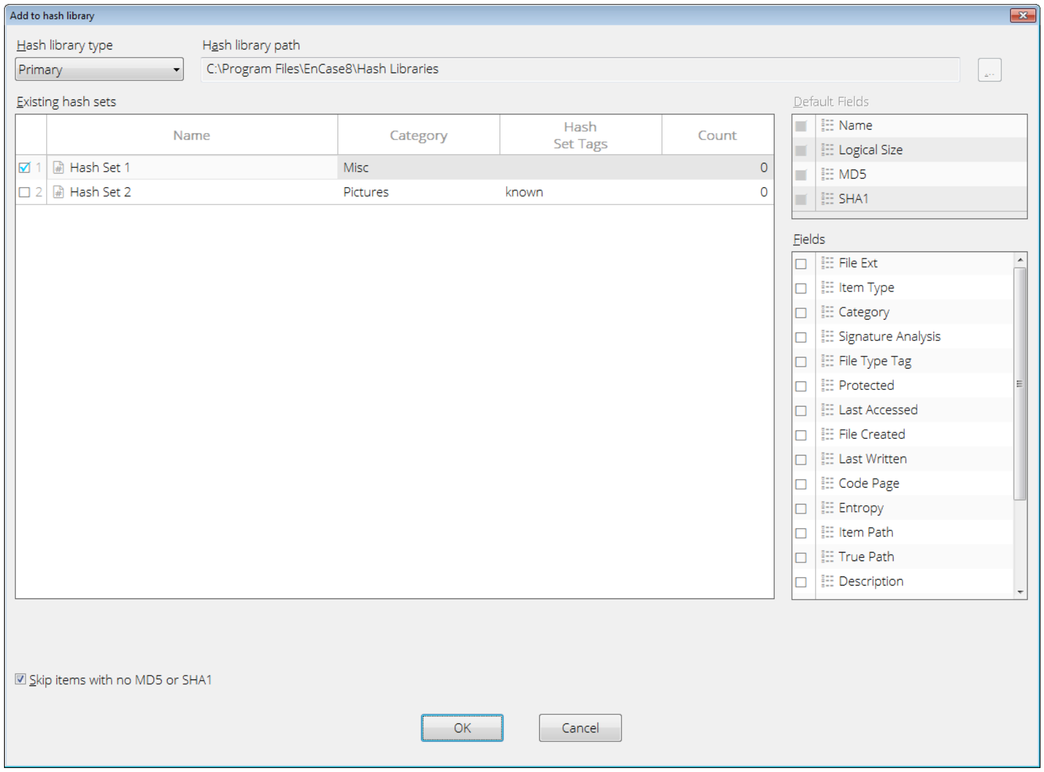
5. When you are prompted to add the new hash set, click **OK**, then click **OK** again. The new hash set is added to the list of ash Sets in the Manage Hash Library dialog.

Adding Hash Values to a Hash Set

After you create a hash set in a library, you can add information to it.

1. Add the device or evidence from which you want to generate a hash value to a case.
2. Hash the files on the device by using the hashing feature of the Evidence Processor or **Hash Individual Files** from the **Entry** > **Entries** menu item.

3. Using the Tree and Table panes, check those entries whose hash values you want to add to the hash set.
4. On the **Evidence** tab, under **Entries** view, click the **Entries** dropdown menu and select **Add to Hash Library**. The Add to Hash Libraries dialog displays.

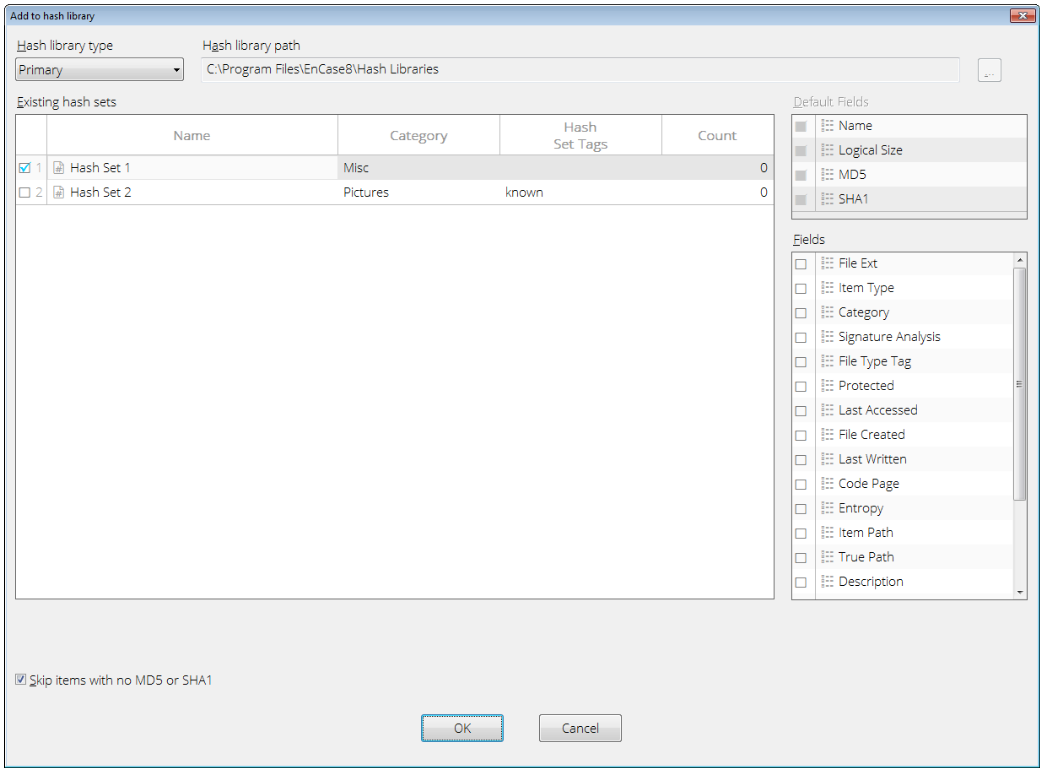


5. Using the **Hash Library Type** dropdown menu, choose the hash library to add the hash items to.
6. Select the **Primary** or **Secondary** hash library (see below for information on setting the Primary and Secondary libraries), or **Other**, if you need to place the item in a different library.
7. After you have selected a library, select one or more previously created hash sets (by checking their boxes) from the **Existing Hash Sets** dialog. If you need to create a new hash set, right click in the **Existing Hash Sets** table and select **New Hash Set**. The **New Hash Set** dialog displays.
8. In the **Fields** list, select the metadata fields you want to add to the hash library for the selected items. Some fields are added by default; however, you can add other optional fields. All fields added to the hash set are reported when a hash comparison matches a particular hash set.
9. Click the **Skip items with no MD5 or SHA1** checkbox to skip all blank items and allow the import to proceed without manually locating and deselecting files with no hash values.
10. When you finish, click **OK**.

Note: Adding additional fields does not increase the comparison time, but does increase the size of the library.

Adding Results to a Hash Library

1. In the results list, check the items you want to add to a hash library.
2. In the Results dropdown menu, click **Add Results to Hash Library**.
3. The Add Results to Hash Library dialog displays.



4. In the Hash Library Type dropdown menu, choose the hash library (**Primary**, **Secondary**, or **Other**) where you want to add results.
5. Select one or more previously created hash sets from the **Existing Hash Sets** list.
6. The Name, Logical Size, MD5, and SHA1 fields are included by default. Select any additional metadata fields you want to add to the hash library for the selected items from the **Fields** list. All fields added to the hash set will be reported when a hash comparison matches a particular hash set.
7. Click the **Skip items with no MD5 or SHA1** checkbox to skip items with no MD5 or SHA1 available and allow the import to proceed without manually locating and deselecting files

with no hash values.

8. When you finish, click **OK**.

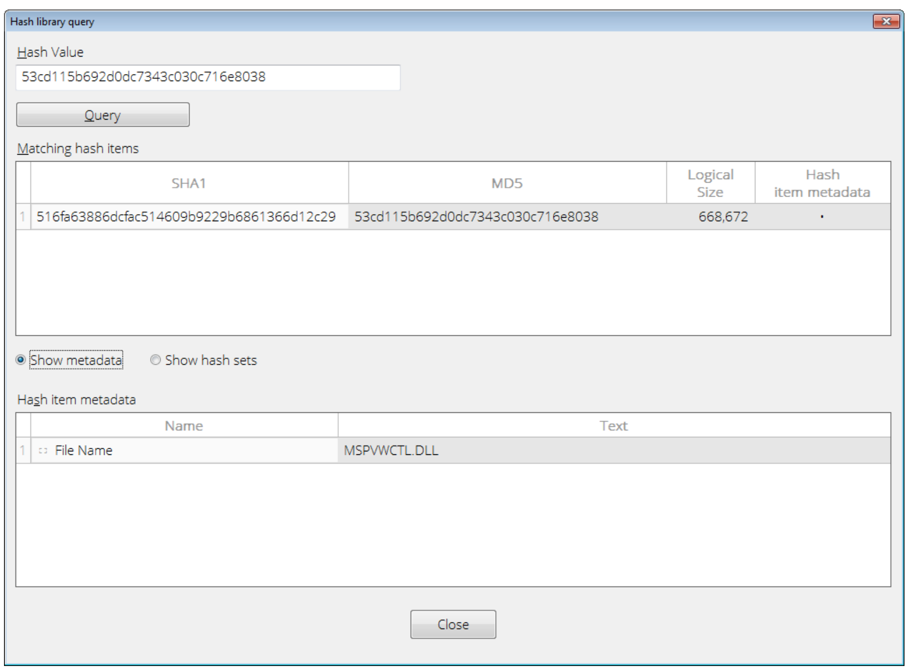
Note: Adding additional fields does not increase the comparison time, but it does increase the size of the library.

Querying a Hash Library

At times, an examiner may want to query a hash library for a particular hash value to verify its existence and to examine the metadata that exists with that value.

To conduct a query of a known hash value:

1. On the home page, click **Tools** > **Manage Hash Library** > **Open Hash Library**.
2. Use the existing hash library, or click the browse button and select a different hash library and click **OK**.
3. The Manage Hash Library dialog lists the hash sets in the hash library.
4. Click **Query All**. The Hash Library Query dialog displays.
5. Paste the value into the **Hash Value** field and click **Query**. Any matches display in the **Matching hash items** table.



6. To obtain more detailed information about the matched hash item, click either **Show Metadata** or **Show Hash Sets**.

Adding Hash Libraries to a Case

After you create one or more hash libraries and add hash sets and hash values to them, you need to associate them with your case.

To associate hash libraries with a case:

1. On the Case home page, click **Case** > **Hash Libraries**.
2. The **Hash Library Info** dialog displays the location of the primary and secondary hash libraries. EnCase can use two hash libraries simultaneously so that you can use a local library as well as a shared library.
3. To set the primary hash library, click the **Primary** row in the table and select **Change Hash Library** in the menu, or double click in the **Hash Library Path** cell next to **Primary**. Browse to the folder containing the hash library.
4. To enable the library, confirm that the **Enable** checkbox is checked for the primary library.
5. The Existing hash sets table displays a list of the hash sets in the selected library. To enable sets, check the **Enable** checkbox.
6. To manage the secondary hash library, select the **Secondary** column and follow the same steps.
7. After you define a primary or secondary hash library, you can manage that library: select it in the table and click **Manage Hash Library** in the toolbar.

> **Note:** EnCase can automatically add a hash library to a case after the hash library is associated with a case. EnCase prompts you with an option to associate the hash library you select with the case that is currently open.

Viewing Hash Sets Associated with an Entry

You can view hash set names associated with an entry in the Table pane and in Hash Sets detail view. The top three hash set names for a table entry are listed in the Hash Set Names column in Table pane. You can view the names of all hash sets in the Hash Sets detail view.

Hash set names and associations with individual entries are collected in the device cache after you set up primary and secondary hash libraries for a case and process evidence. The top three hash set names are pulled from this cache and display in a column in the Table pane.

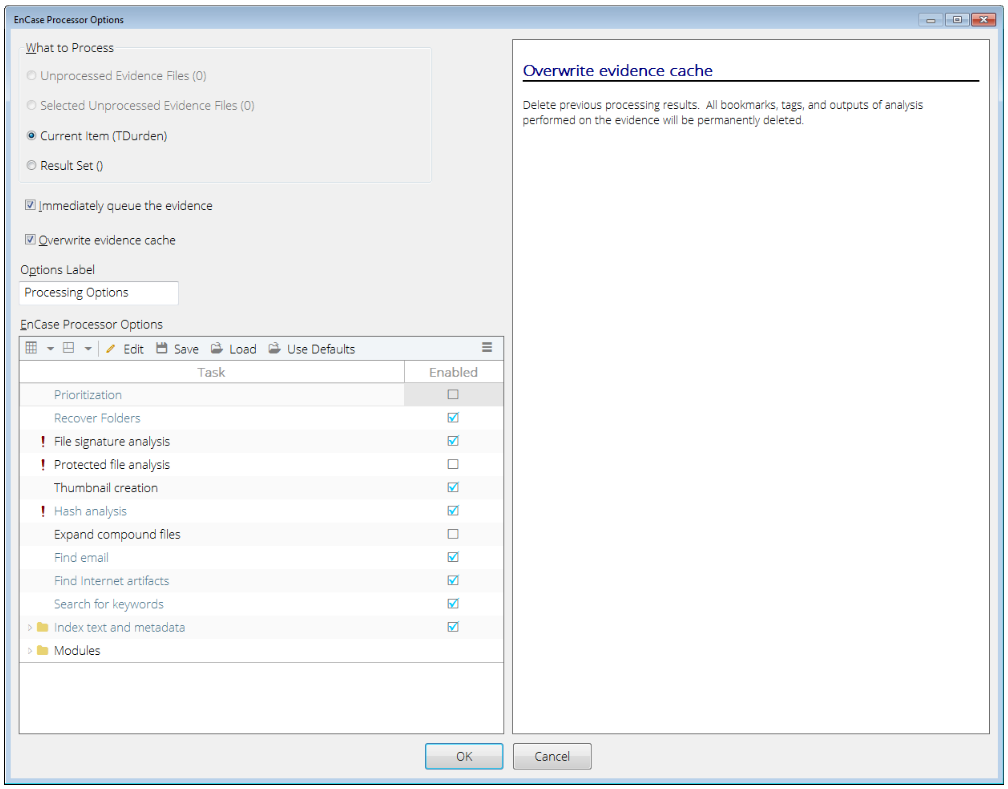
To associate hash sets with entries in the table pane:

1. Set up primary and secondary hash libraries. See Creating a Hash Library on page 282.
2. Select the evidence files for which you want to view associated hash sets.
3. Process the evidence. See Processing Evidence on page 121.

Cache information is preserved until you make a change in the hash library. Reprocessing the evidence updates the hash set associations in the device cache.

To update hash set associations in the device cache:

1. Select the evidence files for which you want to view updated hash set associations.
2. Select **Process** from the Evidence ribbon. The EnCase Processor Options dialog displays.



3. Check the **Overwrite evidence cache** checkbox.
4. Click **OK**.

To view all hash sets associated with an entry:

1. Select the entry from Table pane.
2. Choose **Hash Sets** from the bottom panel ribbon. All hash sets containing the entry display.

Managing Hash Sets and Hash Libraries Associated with a Case

To change hash libraries associated with a case:

1. Click **Case** > **Hash Libraries**.
2. The Hash Libraries dialog displays.
3. Click **Change hash library** on the toolbar to enable or disable hash libraries associated with the current case.
4. Select or clear checkboxes in the Enable column to enable or disable hash sets from the hash library.

Viewing and Deleting Individual Hash Items

The Manage Hash Library function allows you to:

- Select a hash set to work with
- View the contents of a hash set
- Delete individual items from a hash set

Viewing Individual Hash Items

To view individual hash items:

1. From the home page, click **Tools** > **Manage Hash Library**.
2. In the Manage Hash Library dialog, click **Manage Hash Items**. The Viewing (Hash Set) dialog displays.

Deleting Individual Hash Items

To delete individual hash items:

1. In the Viewing (Hash Set) dialog, check the boxes in the Hash Items column you want to delete. This enables the **Delete All Selected** button.
2. Select the items you want to delete, then click **Delete All Selected**.

Changing Categories and Tags for Multiple Hash Sets

When adding hash sets to a hash library, you can specify a hash category and multiple hash set tags for each set. If you want to change these values for a group of hash sets, you can modify them in bulk.

To change the category and tags for multiple hash sets:

1. Click **Tools** > **Manage Hash Library**. The Manage Hash Library dialog displays.
2. Check the boxes next to the hash sets whose values you want to change.
3. Select **Edit Selected** from the Hash Sets menu bar. The Edit Selected dialog displays.
4. Select whether you want to change the existing category or tag for the hash sets, then enter new value in the text box. Click the Hash Set Category checkbox or Hash Set Tags checkbox and enter a new value in the corresponding text boxes.
5. Click **Finish**.

Importing Hash Sets

To import hash sets into an EnCase hash library:

1. On the home page, click **Tools** > **Manage Hash Library**.
2. Click **Import** > **Current Hash Sets...** and browse to the location of the hash set you want to import. The hash set files must be in EnCase's proprietary format with a file extension of BIN.
3. Click **Finish**.

Importing EnCase Legacy Hash Sets

You can import legacy hash sets from versions of EnCase prior to Version 8 into a Version 8 hash library.

1. On the home page, click **Tools** > **Manage Hash Library**.
2. Click **Import** > **EnCase Legacy Hash Sets...** and browse to the location of the hash set you want to import. The filename format must be the EnCase Version 6 hash set format: `[hash set name].Hash`.
3. Click **Finish**.

Importing HashKeeper Hash Sets

You can import legacy hash sets from versions of EnCase prior to Version 8 into a Version 8 hash library.

1. On the home page, click **Tools** > **Manage Hash Library**.
2. Click **Import** > **HashKeeper...** and enter HashKeeper Key and HashKeeper Hash values.
3. Click **Finish**.

NSRL Hash Sets

You can use the centralized National Software Reference Library (NSRL) Reference Data Set (RDS) with EnCase.

The latest version of NSRL RDS is available for download directly from the National Institute of Standards and Technology in EnCase format via this link: http://www.nsrl.nist.gov/Downloads.htm.

Integration with Project VIC

Project VIC (www.projectVIC.org) was created to develop an ecosystem of information and data sharing between law enforcement agencies all working on crimes facilitated against children. Project VIC's mission is to aid law enforcement officers in victim identification by leveraging the use of extremely large and high quality hash sets to identify and eliminate images. There are two ways EnCase Forensic interacts with Project VIC data. You can:

- Check case information against the Project VIC hash library by:
  - Downloading the hash library
  - Importing the hash library into EnCase
  - Applying the hash library to your case
  - Performing hash analysis
- Export images and a .JSON file compatible with Project VIC

OBTAIN THE PROJECT VIC HASH SET .JSON FILE

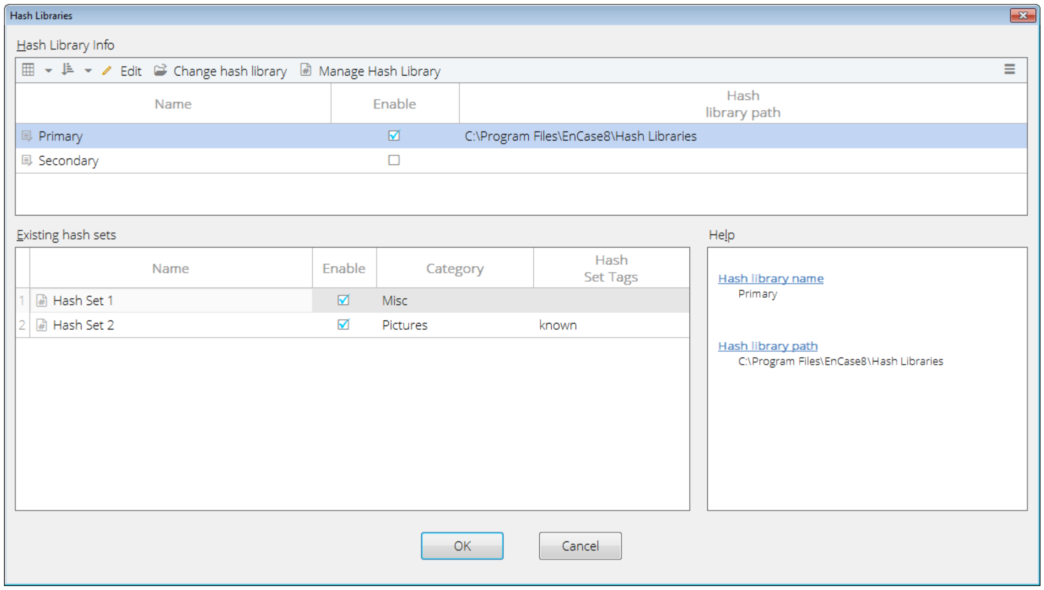
You must be registered with the Internet Crimes Against Children Child Online Protective Services (ICACCOPS) to access the Project VIC hash library. The Project VIC hash library can be downloaded through the Hubstream (www.hubstream.net) Intelligence Agent. The data is saved as a Javascript Object Notation (.JSON) file on your machine.

IMPORT THE PROJECT VIC HASH LIBRARY INTO ENCASE

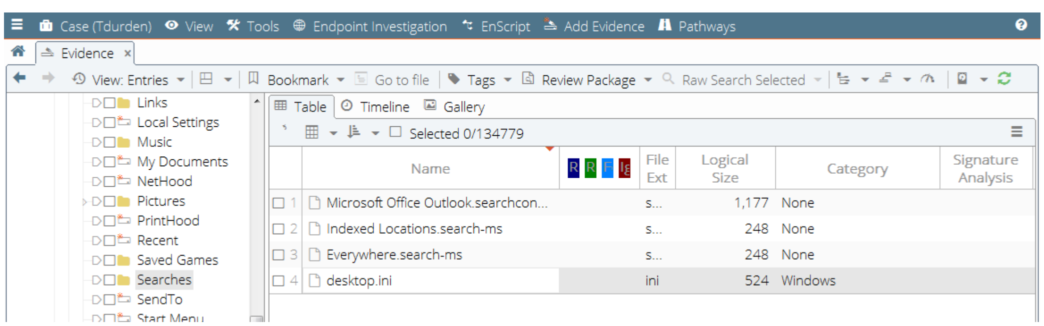
1. Click **Tools** > **Manage Hash Library**. The Manage Hash Library dialog displays.
2. Click **New** and create a new folder in which to store the Project VIC hash library.
3. Click **OK**, then click **Import** > **Project VIC**. The Project VIC dialog displays.
4. Browse to the .JSON file and click **Open**.
5. Click **Finish**. The Project VIC hash sets display in the Manage Hash Set dialog.
6. Click **Close**.

APPLY THE PROJECT VIC HASH LIBRARY TO YOUR CASE

1. Open the case where you want to apply the Project VIC hash library.
2. Click **Case (`Case Name`)** > **Hash Libraries**.
3. The Hash Libraries dialog displays.



4. Double click **Primary** or **Secondary**. In the Browse for Folder dialog, navigate to the Project VIC hash library folder you created and click **OK**. The Existing hash sets area of the Hash Libraries dialog populates with the Project VIC hash sets. Click **OK**.
5. A prompt displays, informing you that you will need to manually run a hash analysis to update the cache. Click OK to proceed.
6. Click **Yes**.
7. Click **OK** to close the Hash Libraries dialog.
8. Perform a hash analysis (CRTL-SHIFT-H).
9. When processing is finished, the **Refresh** button in the upper right corner of the Evidence Tab is enabled.



10. Click the **Refresh** button. The Tree view updates with the Project VIC hash library applied to the relevant files. Matches display in the Hash Set Names column.

EXPORT IMAGES AND A .JSON FILE COMPATIBLE WITH PROJECT VIC

If you find files you believe would be good candidates for inclusion in the Project VIC hash library, you can export them.

1. Blue check the item(s) you want to export.
2. Click **Entries** > **Export Project VIC Files**.
3. Enter or browse to an export path, then click **OK** to generate a .JSON file.
4. You can download this file to Griffeye (www.griffeye.com) where you can further categorize the data or upload it directly to Project VIC using the Hubstream Intelligence Agent. Your file will be reviewed and, if accepted, added to the Project VIC hash library.

CHAPTER 10

BOOKMARKING ITEMS

Overview	297
Working with Bookmark Types	297
Bookmarking Pictures in Gallery View	306
Bookmarking a Document as an Image	307
Working with Bookmark Folders	307
Editing Bookmark Content	309
Decoding Data	310

Overview

EnCase allows files, sections of file content belonging to different data types, and data structures to be selected, annotated, and stored in a special set of folders. These marked data items are bookmarks, and the folders where they are stored are bookmark folders.

EnCase stores bookmarks in `.case` files, and also stores metadata and content associated with a bookmark in the actual bookmark.

Bookmarks and the organization of their folders are essential to creating a solid and presentable body of case evidence. You can examine bookmarks closely for their value as case evidence, and additionally, use the bookmark folders and their data items to create case reports. For more information, see Generating Reports on page 387.

Working with Bookmark Types

EnCase provides several types of bookmarks.

Highlighted Data or Sweeping Bookmarks

The highlighted data bookmark, also known as a sweeping bookmark, defines either:

- An expanse of raw text within a file or document. The raw text is usually a portion of ASCII or Unicode text, or a hexadecimal string.
- A data structure. Data structure bookmarks mark evidence items of particular data interpretation types.

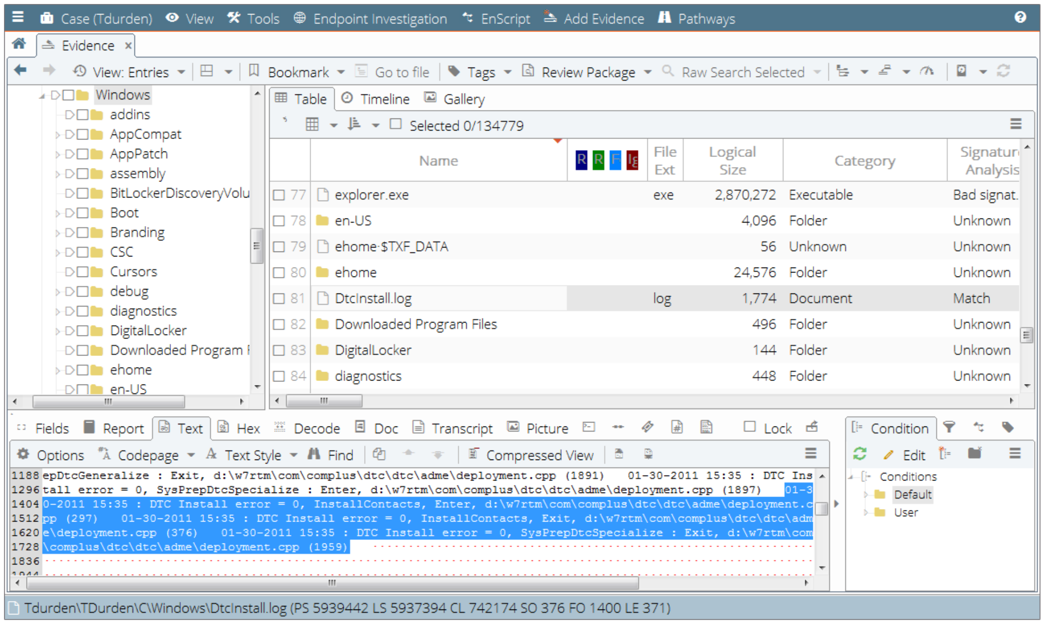
> **Note:** If there is an allocated file associated with a deleted, overwritten file, both files are bookmarked.

Raw Text Bookmarks

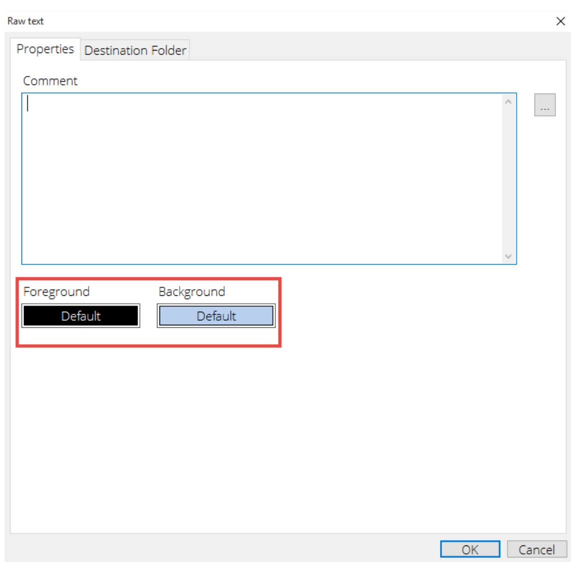
You create raw text bookmarks in EnCase by clicking and dragging raw text in the View pane, just as you would drag-click to highlight content in a text editor. This is done from the **Text** or **Hex** tabs of the View pane.

To create a raw text sweeping bookmark:

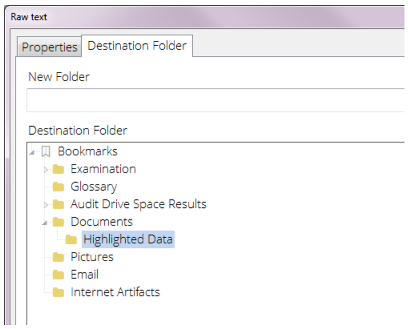
1. In the **Evidence** tab, go to the Table pane and select the file containing the content you want to bookmark.
2. In the View pane, click the appropriate tab (**Text** or **Hex**).
3. Highlight the raw text you want to bookmark.



4. On the menu bar, click **Bookmark** > **Raw text** or right click the highlighted text and click **Bookmark** > **Raw text**.
5. The Raw Text dialog displays. Type some identifying text in the **Comments** box on the **Properties** tab that makes it easy to identify the bookmarked content. If desired, you can highlight a string, create a bookmark, and then highlight a separate string with a different color and create it as a separate bookmark.



6. Click the **Destination Folder** tab to display the bookmark folder hierarchy for the current case, then click the bookmark folder where you want to place this sweeping bookmark. In the example below, the **Highlighted Data** subfolder is selected. Note that you can always rename bookmark folders or move the bookmark later.



7. Click **OK** to create the bookmarked content in the highlighted folder.

Data Structure Bookmarks

Data structure bookmarks mark items such as a Windows partition entry, a Unix text date, or Base64 encoded text. This section describes one example of creating a sweeping data structure bookmark on a date/time data item.

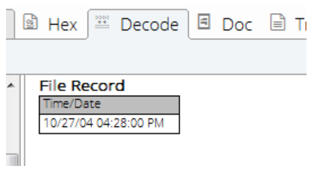
To create a data structure bookmark:

1. Select the evidence item of interest from the Table pane of the **Evidence** tab.
2. Examine the file content in the View pane by clicking the **Text** or **Hex** tab. As an example, let's assume that characters displayed in the pane are not in an easily readable format. Select the bytes of interest.
3. Click the **Decode** tab in the lower right pane.
   - The Quick View decoder enables you to view common decode interpretations in one screen.
     - When populating the Quick View table, all bytes required to successfully interpret the data are read.
     - For example, if one byte is selected, and four bytes are required to decode a 32-bit integer, Quick View looks at the next three bytes to provide the decoded interpretations.
   - The View Types list displays specific decoded values, organized in a tree structure.
     - With the exception of pictures, when viewing by Type, only the selected bytes are interpreted.
     - For example, if one byte is selected, and four bytes are required to decode a 32-bit integer, a decoded interpretation is not available.

- EnCase Forensic attempts to decode pictures from the selected starting byte. The bytes for the entire picture do not need to be selected.

4. Use the Quick View or the View Types lists to investigate the data. To investigate date/-time data, expand the **Dates** folder.

5. For this example, the **HFS Plus Date** option yields a satisfactory interpretation of the data.



6. To bookmark the data, click the **Bookmark** toolbar button. The Data Structure dialog displays.
7. In the Data Structure dialog, type text about the data structure bookmark in the **Comments** box and click the **Destination Folder** tab.
8. In the **Destination Folder** box, click the folder where you want to store this data structure bookmark.
9. Click **OK**.

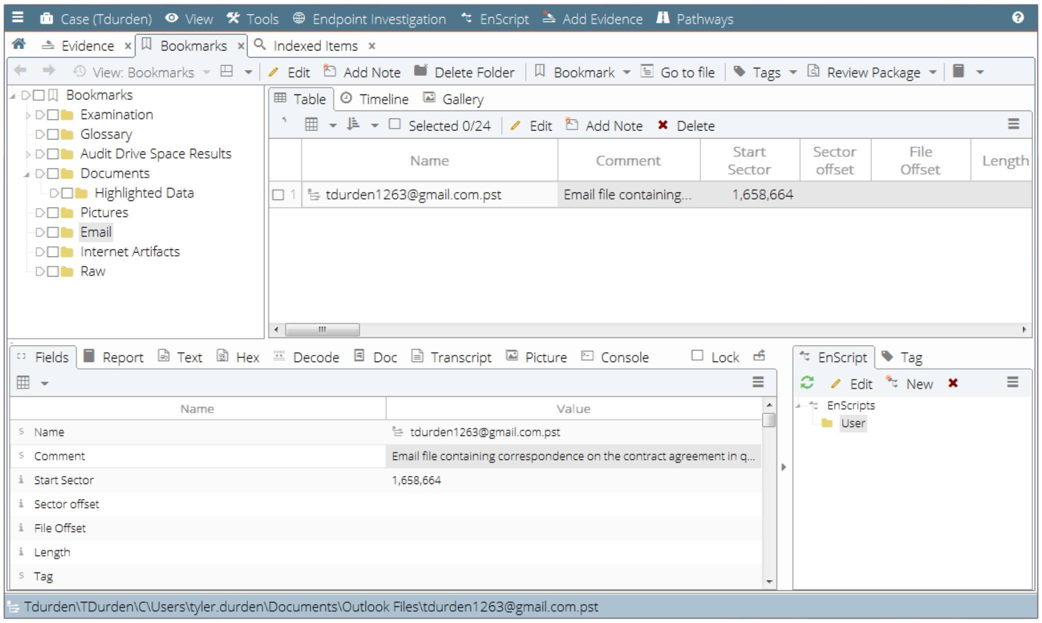
Notable File Bookmarks

Use notable file bookmarks to mark one or more files. You can assign notable files into a bookmark folder either singly or as a selection of files.

Single Notable File Bookmarks

To bookmark a single notable file:

1. From the appropriate tab, select the file of interest in the Table pane by clicking its row. In the example below, a `.pst` file is selected.



2. On the toolbar, click **Bookmark** > **Single item**.
3. The Single item dialog opens. On the **Properties** tab, type some identifying text in the **Comment**. Alternatively, you can use the browse button to view a list of existing comments, and select one of those.
4. Click the **Destination Folder** tab to display the case's bookmark folder hierarchy. Click the bookmark folder where you want to store the bookmark.
5. Click **OK**.

Multiple Notable Files Bookmarks

You can also select a group of notable files to bookmark. This feature allows you to quickly store a collection of notable files into a bookmark folder, which can contain other bookmarks.

> **Note:** You cannot use this bookmark selection with sweeping bookmarks.

To bookmark a selection of notable files:

1. In the Table pane, select two or more files. When selecting multiple files in the Table pane, use the checkboxes beside the files.
2. On the toolbar, click **Bookmark** > **Selected items**
3. The Selected items dialog opens. Type some identifying text in the **Comment** box on the **Properties** tab that describes the file. You can also use the browse button to view a list of existing comments, and use one of those.
4. Click the **Destination Folder** tab to display the case's bookmark folder hierarchy, and click the bookmark folder where you want to store the bookmarks.
5. Click **OK**.

Bookmarking Case Analyzer Data

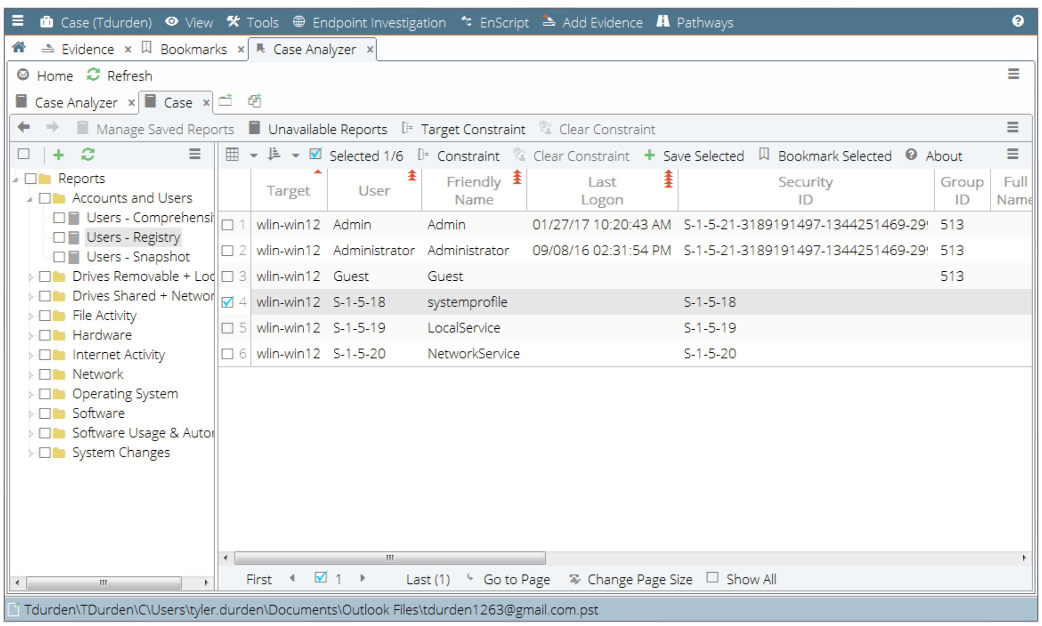
OVERVIEW

You can Bookmark all artifacts and items associated with a Case Analyzer report directly from Case Analyzer.

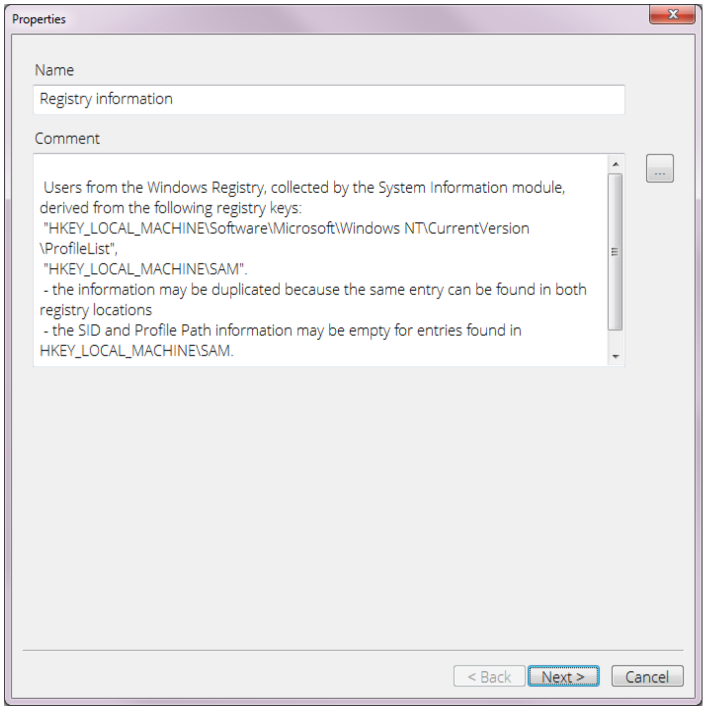
BOOKMARKING PROCESS

Follow these steps to create a Bookmark in Case Analyzer.

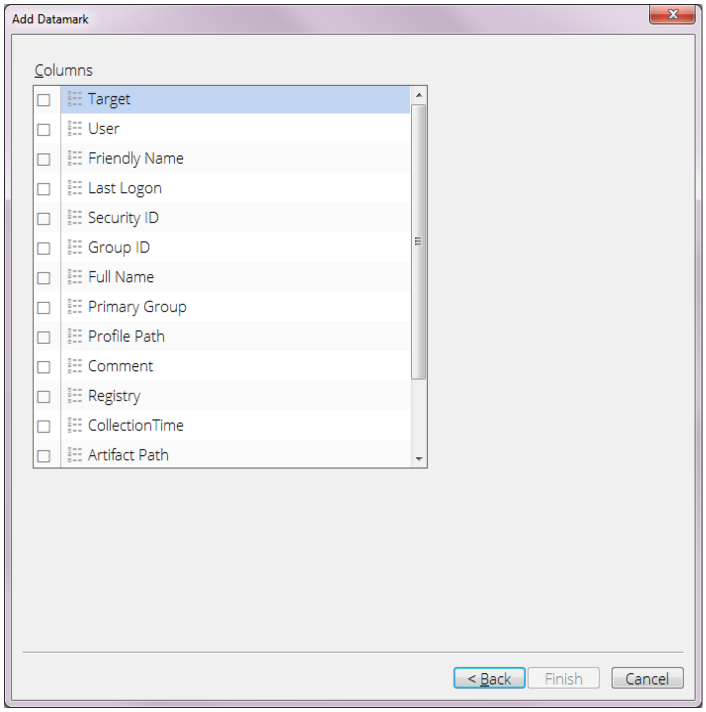
1. In the Case Analyzer **Case** tab, select a report.
2. Select one or more rows in the table window on the right.
3. Click **Bookmark Selected**. This adds a bookmark to the case, bookmarking the selected artifacts.



4. The Properties dialog displays.



5. Enter a name for the Bookmark or accept the default. The Bookmark name is the name of the current report, by default.
6. Enter a comment or accept the default. Each comment includes information on the source of the bookmarked data. The Comment text defaults to the text shown when you click **About** for the current report.
7. The Destination Folder dialog displays.
8. Select a destination folder for the Bookmark or create a new folder. Click **Next**.
9. The Add Datamark dialog displays.



10. Select a column to categorize the Bookmark. The Bookmark displays in this column in the final report.
11. Click **Finish**. EnCase adds the new Bookmark to the case.

Table Bookmarks

You can select a table to bookmark. Highlight a table and select it as a Table bookmark in order to save its metadata and store it in a bookmark folder. Table bookmarks are especially useful for representing evidence data in reports.

Transcript Bookmarks

If the **Transcript** tab in the Viewer pane is active, you can bookmark transcript text.

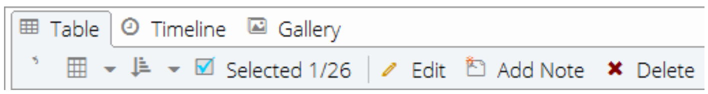
The **Transcript** tab extracts text from a file containing mixtures of text and formatting or graphic characters. The transcript view is useful for creating bookmarks inside files that are not normally stored as plain text, such as Excel spreadsheets.

Notes Bookmarks

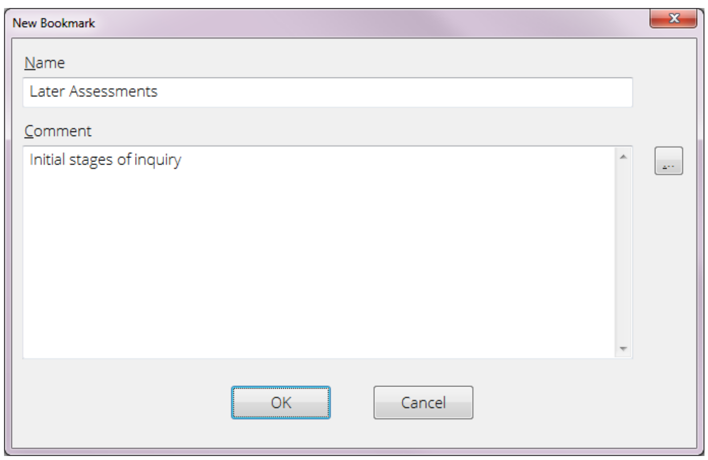
Notes differ from other bookmarks in that you use them with other bookmarks to annotate report data. They do not mark distinct evidence items like other types of bookmarks. A notes bookmark has a field reserved only for comment text that can hold up to 1000 characters.

To create a notes bookmark:

1. Click the **Bookmarks** tab.
2. On the Table toolbar, click **Add Note**.



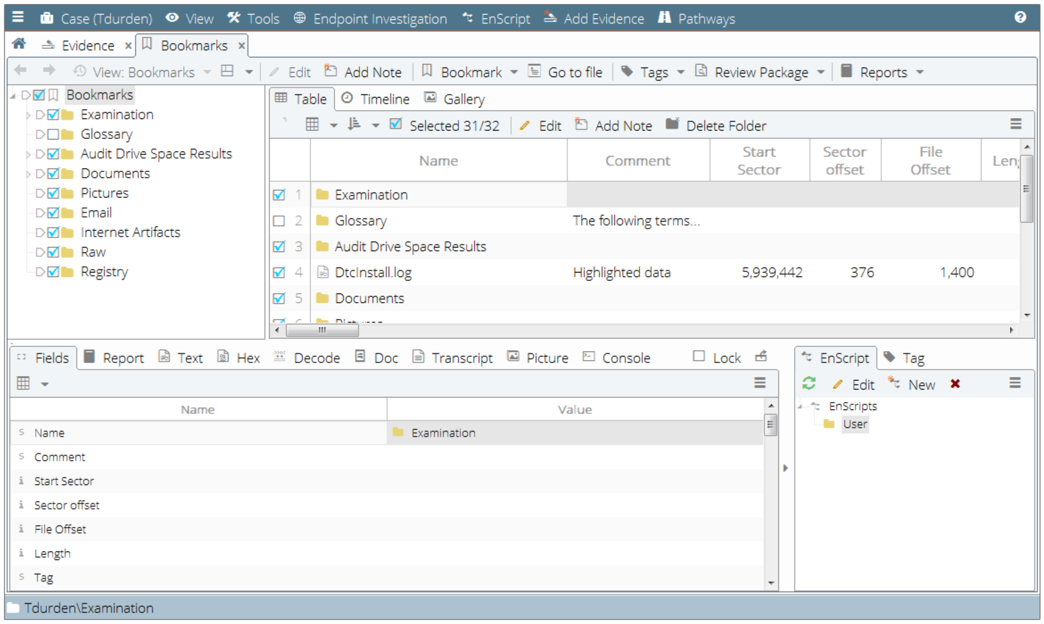
3. The **New Bookmark** dialog opens.



4. Type a **Name** for the note bookmark, then type text in the **Comment** box or browse for a list of previous comments. This is the bookmark text where the note is added.
5. Click **OK**.

Viewing Notes Bookmarks

If you display note bookmarks (**Bookmarks** > **Table**) in Tree-Table view, each displays as a data row in a flattened bookmark hierarchy.



To show the notes in their true order in the bookmark folder hierarchy, click **Split Mode** on the Bookmark toolbar and select **Traeble** view.

Use the **Report** tab in the View pane to show how the note actually displays in reports, as shown above.

Bookmarking Pictures in Gallery View

One of the most frequent uses for bookmarking items is to bookmark pictures or photos in **Gallery** view. The procedure for bookmarking pictures is almost the same as bookmarking single or multiple notable file items.

To bookmark a picture in Gallery view:

1. Click the **Gallery** tab and browse through the pictures.
2. Right click the image to be bookmarked and click **Bookmark** > **Single item...**
3. The Single item dialog opens. On the **Properties** tab, type identifying text in the **Comment** box.
4. Click the **Destination Folder** tab to display the case's bookmark folder hierarchy. Click the bookmark folder where you want to store the bookmark.
5. Click **OK**.

Bookmarking a Document as an Image

You can bookmark Microsoft Office, PDFs, or OpenOffice documents as images that can be inserted into reports with formatting and pagination intact. Microsoft Excel spreadsheet pages and orientation cannot be modified.

To bookmark a document as an image:

1. While in the Evidence tab, select the document you want to bookmark from your evidence list and click the **Doc** tab in the lower view pane.
2. In the Doc tab, select Bookmark Page as Image. A dialog opens, displaying all the pages in the selected document.
3. Select the page(s) you want to create as an image, and click **Next**.
4. Add an optional comment, and click **Next**.
5. Select a folder in which to add the image and click **Finish**.

The image is added to all appropriate reports automatically. Original formatting and pagination, when available, is preserved.

Working with Bookmark Folders

The bookmark folder structure is essential for organizing your bookmarks. You have a great deal of flexibility in creating a folder structure that suits a particular case.

Bookmark folders are organized according to a standard tree structure, with a folder named "Bookmark" at the top the hierarchy. The various bookmark folders (and subfolders) are beneath this node.

If you are not using the default bookmark folders, assign bookmark folder names that identify their content or are meaningful to your case team. For example, you can organize the folders by type of computer evidence, or by relevance to a particular part of the case.

> **Note:** Bookmark folders are nonspecific in nature. Any default folder or folder you create can hold any data type or content.

Bookmarking Template Folders

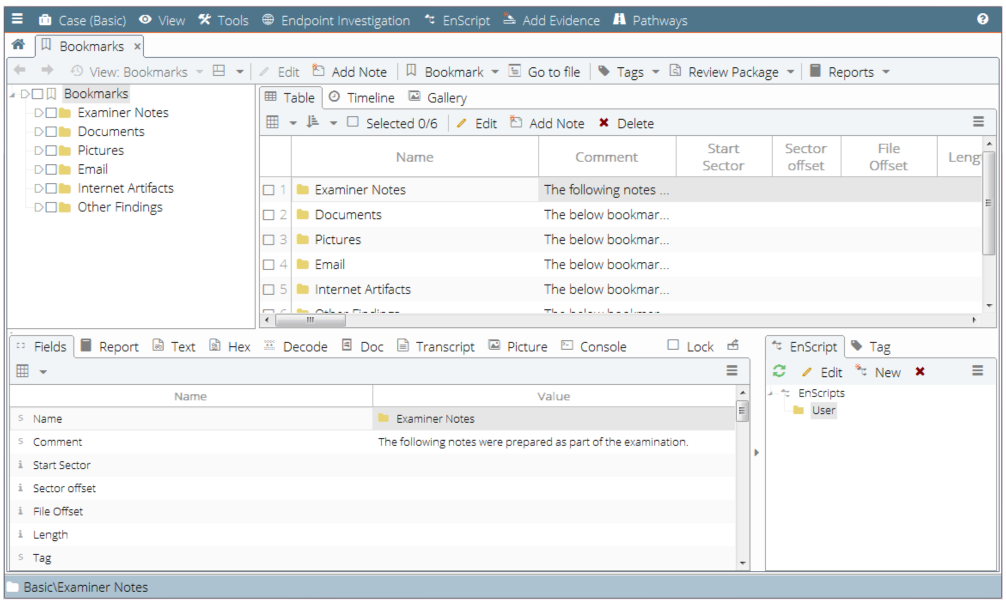
Cases created from EnCase supplied templates, such as the **#Basic** template, include a selection of default bookmark folders. Guidance Software provides the **#Basic** template and the **#Forensic** template. Depending on your needs, you may want to choose one of these

when creating a new case from the Case Options dialog.

To display the set of default bookmark folders for the **#Basic** template, start a case and choose the **#Basic** template.

To view the bookmark folders included in the template:

1. Click **View** > **Bookmarks**.
2. In the **Bookmarks** tab, the Bookmarks root node folder displays at the top of the tree pane.
3. To expand the **Bookmarks** folder, click its tab. This displays the default bookmark folders (shown both in the Tree and Table panes).



Guidance Software recommends using the supplied labels for the bookmark folders to organize the types of bookmarked content (Documents, Pictures, Email, and Internet Artifacts). Although this folder organization is entirely flexible, bookmark folders are directly linked to the Report template that is also included in the default templates. If a case grows to where it needs more bookmark folders or a greater level of bookmark organization, you can create new folders or modify the folder organization, but you may need to make changes to the Report template.

Creating New Bookmark Folders

You can create new folders and subfolders at different levels of the bookmark folder hierarchy.

To create a new bookmark folder:

1. In the Tree pane, right click the **Bookmark** root folder.
2. Click **New Folder...**
3. A new folder displays one level beneath the **Bookmark** root folder highlighted in blue.
4. Type a name for the folder and click **Enter**.
5. To create a new subfolder, repeat the process at the folder level.

Editing Bookmark Folders

To edit a bookmark folder:

1. Click the **Bookmark** tab to display the tree of bookmark folders.
2. Select the bookmark folder you want to edit, right click to display its context menu and click **Edit**.
3. The **Edit <"Folder Name">** dialog displays.
4. Edit either **Name** or **Comment** for the bookmark folder, or both, and click **OK**.

Deleting Bookmark Folders

To delete a bookmark folder:

1. In the Tree view of the **Bookmark** tab, click the **Bookmark** folder you want to delete.
2. Right click the folder and click **Delete Folder...**. A delete confirmation prompt displays.
3. Click **Yes** to delete the folder. Use caution, since deleting a bookmark folder also deletes any bookmarked items in the folder.

Note: Deleting a bookmark folder also deletes any bookmarked items in the folder.

Editing Bookmark Content

You can edit most bookmark categories via the right click context menu or by double clicking the bookmark.

Editing Bookmarks

To edit a bookmark:

1. Click **Edit...** and modify the text in the **Comments** box of the **Properties** tab.
2. You can also click the browse button (**...**) in the dialog to view a list of bookmark comments.
3. Select a comment from the list to replace the current comment.
4. Click **OK**.

Renaming Bookmarks

To rename a bookmark:

1. From the Home page, click **View** > **Bookmarks**.
2. In the **Table** pane, find the bookmark folder with the bookmark you want to rename.
3. The Table pane displays the list of bookmarks for the selected folder. Select the cell for the bookmark to rename.
4. Right click the bookmark folder or the cell you want to rename.
5. Click **Rename**. The bookmark name is highlighted.
6. Enter a new name for the bookmark and click **OK**.

Decoding Data

You can see decoded interpretations of your evidence, when viewing it in text or hex format, using the **Decode** tab in the lower right pane of the **Evidence** pane.

1. On the **Text** or **Hex** tabs in the **View** pane, select the bytes you want to decode.
2. Click the **Decode** tab in the lower right pane and select from the list of decoding options.
3. View the decoded interpretations of your evidence:

    - The Quick View decoder enables you to view common decode interpretations in one screen.
        - When populating the Quick View table, all bytes required to successfully interpret the data are read.
        - For example, if one byte is selected, and four bytes are required to decode a 32-bit integer, Quick View looks at the next three bytes to provide the decoded interpretations.

    - The View Types list displays specific decoded values, organized in a tree structure.
        - With the exception of pictures, when viewing by Type, only the selected bytes are interpreted.
        - For example, if one byte is selected, and four bytes are required to decode a 32-bit integer, a decoded interpretation is not available.
        - EnCase Forensic attempts to decode pictures from the selected starting byte. The bytes for the entire picture do not need to be selected.

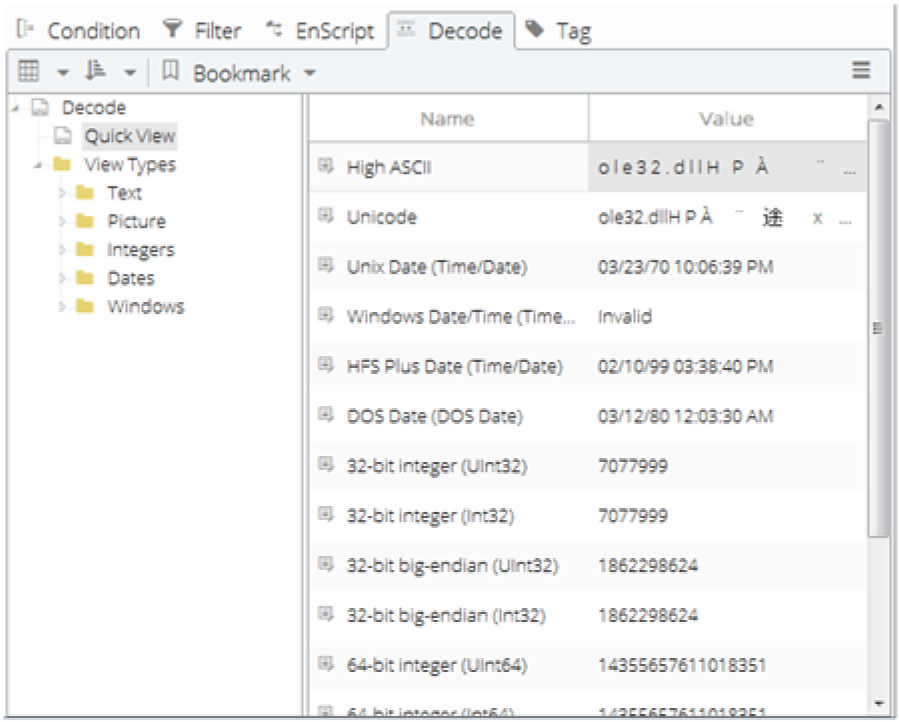
4. To bookmark your selection:

    - From Quick View, right click and select **Bookmark**.
    - From the View Types list, click the **Bookmark** button.

Quickly Viewing Decoded Data

The Quick View decoder enables you to view common decode interpretations in one screen.

- When populating the Quick View table, all bytes required to successfully interpret the data are read.
- For example, if one byte is selected, and four bytes are required to decode a 32-bit integer, Quick View looks at the next three bytes to provide the decoded interpretations.



Viewing Decoded Data by Type

When viewing decoded data by type, each decoded interpretation may be seen individually:

Text

The Text folder contains child objects for formatting which you can use when displaying bookmarked content as text.

- **Do not Show** hides the content of the bookmark.
- **High ASCII** displays the text in 256-bit ASCII.
- **Low ASCII** displays the text in 128-bit ASCII.
- **Hex** displays the text as hexadecimal digits, rather than characters.
- **Unicode** displays the text in Unicode (UTF-16).

- **ROT 13 Encoding** decodes ROT 13 encoded text to ASCII text.
- **Base64 Encoding** decodes Base64 encoded text to ASCII text.
- **UUE Encoded** decodes UUE encoded text to ASCII text.
- **Quoted Printable** is an encoding using printable ASCII characters and the equals (=) sign to transmit 8-bit data over a 7-bit data path.
- **HTML** decodes HTML into text.
- **HTML (Unicode)** decodes Unicode HTML into text.

Pictures

The Pictures data types display data as images.

- **Picture** displays images.
- **Base64 Encoded Picture** displays Base64 encoded images.
- **UUE Encoded Picture** displays UUE encoded images.

Integers

The Integers data types include these categories:

- **8-bit** displays the bookmarked content as 8-bit integers.
- **16-bit** displays the bookmarked content as 16-bit Little-Endian integers.
- **16-bit Big Endian** displays the bookmarked content as 16-bit Big-Endian integers.
- **32-bit** displays the bookmarked content as 32-bit Little-Endian integers.
- **32-bit Big Endian** displays the bookmarked content as 32-bit Big-Endian integers.
- **64-bit** displays the bookmarked content as 64-bit Little-Endian integers.
- **64-bit Big Endian** displays the bookmarked content as 64-bit Big-Endian integers.

Dates

The Dates data types include these categories:

- **DOS Date** displays a packed 16-bit value that specifies the month, day, year, and time of day an MS-DOS file was last written to.
- **DOS Date u(GMT)** displays a packed 16-bit value that specifies the time portion of the DOS Date as GMT time.
- **UNIX Date** displays a Unix timestamp in seconds based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT.
- **UNIX Date Big-endian** displays a Unix timestamp in seconds based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT, as Big-Endian integers.
- **UNIX Text Date** displays a Unix timestamp in seconds as text based on the standard Unix epoch of 01/01/1970 at 00:00:00 GMT.

- **HFS Date** displays a numeric value on a Macintosh that specifies the month, day, year, and time when the file was last written to.
- **HFS Plus Date** is an improved version of HFS Date. It displays a numeric value on a Macintosh that specifies the month, day, year, and time when the file was last written to. HFS Plus is also referred to as "Mac Extended."
- **Windows Date/Time** displays a numeric value on a Windows system that specifies the month, day, year, and time when the file was last written to.
- **Windows Date/Time (Localtime)** displays a numeric value on a Windows system for the local time specifying the month, day, year, and time when the file was last written to.
- **OLE Date** displays a date as a double-precision floating point value that counts the time from 30 December 1899 00:00:00.
- **Lotus Date** displays a date from a Lotus Notes database file.

Windows

The Windows data types include these categories:

- **Partition Entry** displays a partition table entry from the Master Boot Record.
- **DOS Directory Entry** displays a DOS directory entry.
- **Win95 Info File Record** displays Recycle Bin details from Windows 9x INFO files.
- **Win2000 Info File Record** displays Recycle Bin details from Windows 2000+ INFO files.
- **GUID** displays a 128-bit globally unique identifier (GUID).
- **UUID** displays a 128-bit universally unique identifier (UUID).
- **SID** displays a Windows Security Identifier (SID).

CHAPTER 11

TAGGING ITEMS

Overview	317
Creating Tags	317
Tagging Items	319
Hot Keys for Tags	319
Viewing Tagged Items	320
Hiding Tags	321
Deleting Tags	321
Changing the Tag Order	322
Select Tagged Items	322

Overview

The EnCase tagging feature lets you mark evidence items for review. You define tags on a per case basis; default tags can be part of a case template.

Any item that you can currently bookmark can also be tagged. You can search for tagged items, view them on the **Search Results** tab, and view the tags associated with a particular item in Evidence or Record view.

Tag features and characteristics give you these capabilities:

- You can create tags as part of a case or add them to a case template, then customize each tag with specific colors and display text.
- You can edit saved tags: change their colors and text, hide specific tags from view, and delete tags.
- You can directly manipulate tags on the EnCase user interface: modify the order in which they display, delete them from the display, and so forth.
- You can build searches based on tags you have created and tag search results. You can also combine tags with index and keyword search queries.
- You can sort the tag column to find items with multiple tags.

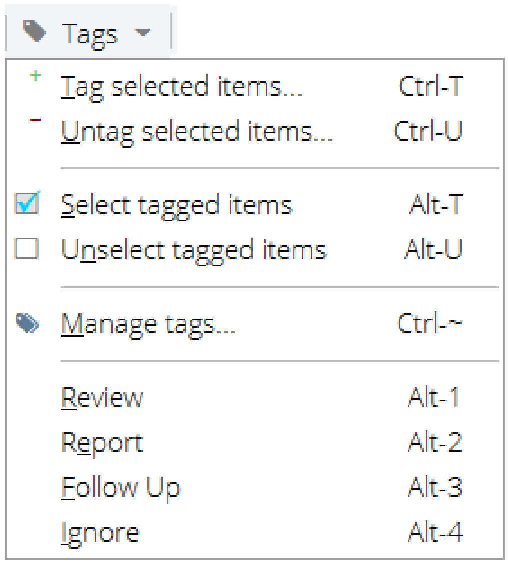
Tags also have these properties:

- Tags are persistent when you are working with entries and when you save and re-open a case.
- Tags are local to a specific case (that is, you cannot create global tags).
- You can create up to 63 unique tags per case.
- Each item, entry, email, or artifact can have multiple tags.

Creating Tags

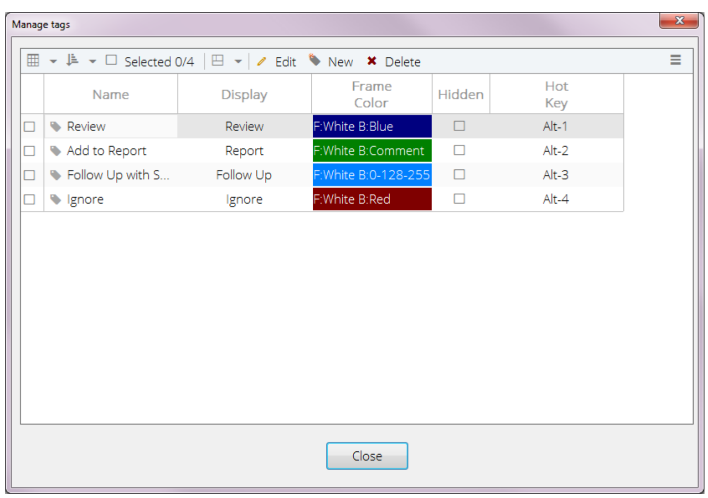
To create a tag:

1. On the **Artifacts**, **Evidence**, or **Bookmark** tab, click **Tags** on the toolbar.
2. On the **Tags** dropdown menu, click **Manage Tags**.



3. On the Manage Tags toolbar, click **New**.
4. On the New Tag Item page, enter:
   - A **Name** for the tag.
   - The **Display Text** that displays in the Tag column (Guidance Software recommends using short display names to conserve space).
   - The **Frame Color** (foreground and background colors) for the tag.
   - You can also hide the tag from displaying by checking the corresponding **Hidden** box.

5. Repeat the preceding two steps until you have created the set of tags you need. You can always add, remove, and rename tags while working on a case.



Tagging Items

To tag an evidence item:

1. On the **Evidence** tab, display your evidence items. (You can also assign tags to **Artifacts, Bookmarks**, and **Results**.)
2. Highlight or check the evidence item to which you want to assign a tag.
3. Display a list of available tags by clicking **Tags** > **Show Tag Pane**. A pane displays in the lower right corner of the EnCase user interface. The pane contains a list of default and custom tags and the number of occurrences of each tag.
4. Check the tag that you want to assign to an evidence item.
5. The tag displays in the Tag column of the selected evidence item.

You can also tag an item by clicking its position in the Tag column:

1. Display a list of available tags by clicking the **Tags** tab from the lower right pane. The order that the tags are shown in the table (top to bottom) corresponds to the order in which they display in the Tag column (from left to right).
2. Click the space in item's Tag column where the tag would be displayed. The tag displays.
3. As an example, if you configured two tags:
   - The left half of the Tag column is used to display the first tag.
   - The right half of the Tag column is used to display the second tag.
4. Click the first half of the tag cell to display the item's first tag, and the second half of the tag cell to display the item's second tag.
5. To remove a tag from displaying, click the tag.

SORTING TAGS

You can sort the entire tag column by individual tag. Clicking the tag name within the tag column header sorts the column by the tag name. Also, clicking the narrow gray area around the tag name, within the tag column, sorts the entire contents of the tag column.

In ascending order, items with a tag in the rightmost column will be sorted first. Items with a tag in the second rightmost column will be sorted second.

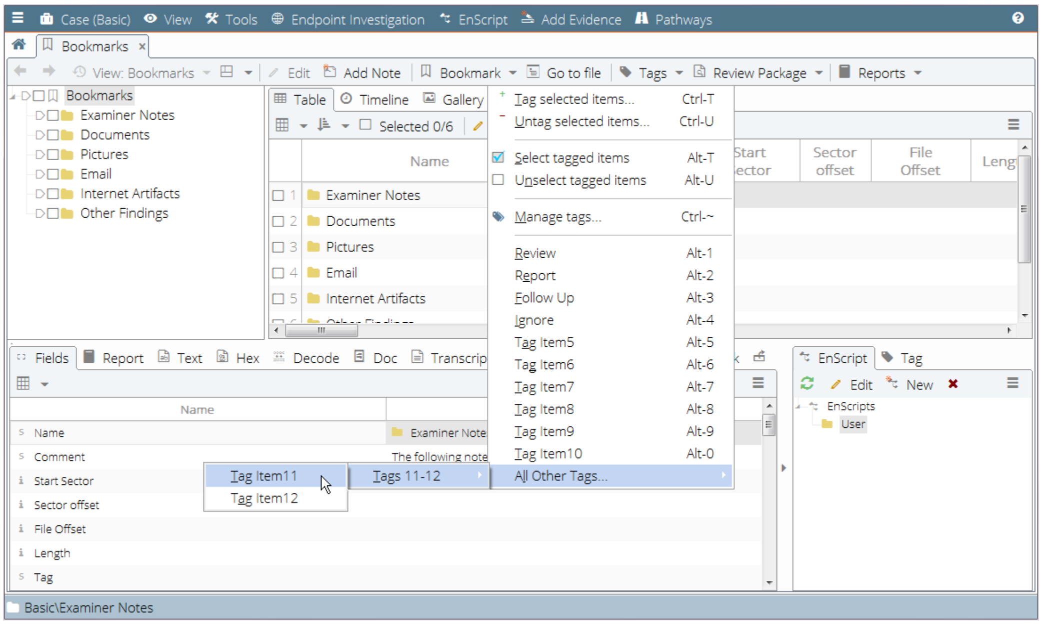
In descending order, items with a tag in the leftmost column will be sorted first. items with a tag in the second leftmost column will be sorted second.

Hot Keys for Tags

You can use keyboard shortcuts to assign tags.

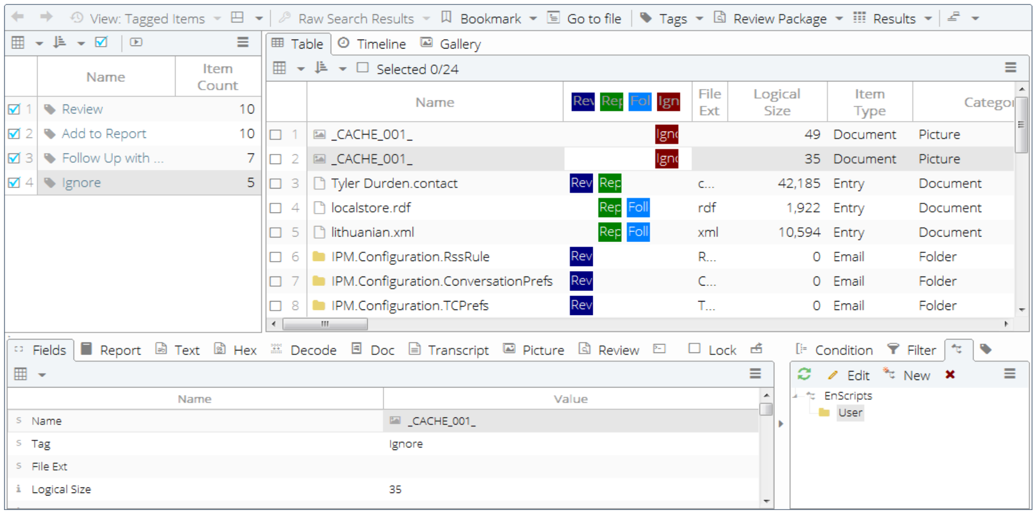
- Hot keys are assigned to the first ten tags in the Tag database.
- The hot keys **Alt-1** through **Alt-9** and **Alt-0** are assigned to the first ten tags.
- Remaining tags can be assigned via the second level menu: **All Other Tags**.
- The maximum number of tags allowed in a case is 63. Using the **Manage Tags** option, you can create additional tags beyond the case limit of 63.

Click the **Tags** dropdown menu to view keyboard shortcuts for tags.



Viewing Tagged Items

The following figure shows the EnCase Tag menu and a portion of a results table with some of the tagged items. Note how the Tag column can display multiple tags, customized with different text and in different colors.



Hiding Tags

You can choose to hide tags in the Tag column or the Tag pane using the Manage Tag dialog. You can also unhide a previously hidden tag in the same way. Hiding a tag prevents it from being displayed without deleting the tag.

To hide or unhide a tag:

1. On the **Evidence** tab, click the **Tags** button.
2. On the Manage Tags dialog, check the box in the **Hidden** column for the tag you want to hide or unhide.

Deleting Tags

You can delete tags from the Manage Tags window. Deleting a tag removes the tag name from the case and deletes all references to the tag in the tag database. This action cannot be undone.

To delete a tag:

1. On the **Evidence** tab, click the **Tags** button. The Manage Tags window displays.
2. Check the row of the tag that you want to delete.
3. Click the **Delete** button on the Manage Tags toolbar.

> **Note:** If the tag is assigned to at least one case item, a warning dialog displays with the number of tags to be deleted. If the no items are tagged, no warning dialog displays.

Changing the Tag Order

For cells with multiple tags, you can change the tag order by dragging individual tags to a new position within the cell.

To change the position of a tag within a cell:

1. Left click on a tag in the cell and hold the mouse button down.
2. Drag the tag to a new position in the cell and release the mouse button.

Select Tagged Items

Tags persist across views, and selected items (that is, blue checks) may not persist across all views in EnCase. Some operations, like performing an acquisition of a logical evidence file, operate only on selected items, and in these cases, it can be useful to select items based on tag assignments.

1. Click **Tags** > **Select tagged items**.
2. The Select Tagged Items dialog displays.
3. Select the tags you want, then click **OK**.

   Note: There are some operations (for example, **Create Logical Evidence File**) that act on selected items only.

CHAPTER 12

USING ENCASE PORTABLE

Overview	325
Creating EnCase Portable Jobs	326
Collecting Evidence	355
Analyzing and Reporting on Data	365
Maintenance	374
Configuring EnCase Portable for NAS Licensing	378
Troubleshooting	379
FAQs	381

Overview

EnCase Portable automates the collection of evidence from computers in the lab and in the field. It is a self-contained application that runs on a removable USB device inserted into a running machine.

EnCase Portable functionality is included in the full EnCase product. It can also be purchased separately as a standalone product to create, manage, run, and analyze jobs.

One or two removable devices are required to execute Portable jobs:

- The Portable device contains and executes preconfigured jobs that collect evidence from target machines.
- When using the standalone version of EnCase Portable, EnCase Portable is executed from the security key.
- Evidence can be stored on the Portable device if desired. However, a separate Portable storage device can be used to collect large amounts of evidence if necessary.

When EnCase Portable is purchased as a standalone product, it comes packaged in a kit containing a Portable device and security key (8 GB Pocket-Sized USB Device).

EnCase Portable can be run using an EnCase Portable security key, or on a prepared Portable device. When EnCase Portable is run from a Portable security key, you can create collection jobs directly on the device. When using Portable functionality from EnCase, you can create collection jobs in EnCase and export them to either a Portable security key or a prepared portable device.

Once the evidence is collected directly on the Portable device or the Portable storage device, it can be analyzed in the field or imported back into EnCase to review the results. You can build and generate reports that capture all or selected parts of the collected information.

The process for evidence collection includes:

1. Create your collection jobs in Portable Management. This can be done from EnCase or on the Portable device itself.
2. If the jobs were created in EnCase, export the jobs to the Portable device.
3. Run the jobs from the Portable device.
4. Analyze the collected data.
5. If you own EnCase, import the evidence you have collected into EnCase.
6. Build and generate reports.

Creating EnCase Portable Jobs

A Portable job consists of a group of settings for collecting specific information.

If EnCase is installed, jobs are typically created in EnCase and exported to the Portable device. You can also create and edit jobs directly from the Portable device. Once a job is created, you can modify or copy it to create other jobs. Some jobs can be configured to triage the information as it comes in, so you can choose exactly what information to collect.

Jobs use modules, which are configurable sets of instructions for how to look for certain kinds of data, such as information found in running memory, certain types of files, etc. Modules also define a specific set of data to be collected. You can configure the information collected by a module by selecting a specific set of options for each module.

SYSTEM MODULES

- The **System Info Parser** module collects system artifacts related to user activity, network configurations, installed software, hardware components, startup routines, user-s/accounts, and shared/mapped drives. This information is pulled from the Windows registry or the system files appropriate to a given Linux distribution.
- The **Windows Artifact Parser** module collects link files, the MFT $LogFile transaction log, and Recycle Bin items.
- The **Encryption** module produces a single page report listing the encryption type of each drive and volume on the target system.

SEARCH MODULES

- The **Personal Information** module collects information containing personal information. This module searches all document, database, and Internet files and identifies Visa, MasterCard, American Express, and Discover card numbers, as well as Social Security numbers, phone numbers, and email addresses. Jobs created with this module enable you to triage information as it is being collected.
- The **Internet Artifacts** module collects a history of visited websites, user cache, book-marks, cookies, and downloaded files.
- The **File Processor** module provides a way to review and collect specific types of files. From within the File Processor module, you can elect to find data using metadata, keywords, or hash sets, or find picture data. You can also configure your own collection sets using an entry conditions dialog. Jobs created with this module enable you to triage information as it is being collected. You can then decide what files, if any, to collect.

LOG PARSER MODULES

- The **Windows Event Log Parser** module collects information pertaining to Windows events logged into system logs, including application, system, and security logs.
- The **Unix Login** module parses the Unix system WTMP and UTMP files, which record all login activities.
- The **Linux Syslog Parser** module collects and parses Linux system log files and their system messages.

COLLECTION MODULES

- The **Snapshot** module collects a snapshot of pertinent machine information. Captured information includes running processes, open ports, logged on users, device drives, Windows services, network interfaces, and job information.
- The **Acquisition** module acquires drives and memory from target machines.
- The **Screen Capture** module preserves images of each open window on a running machine.

Creating Jobs

You can create a job either from within EnCase or from the Portable device when in the field.

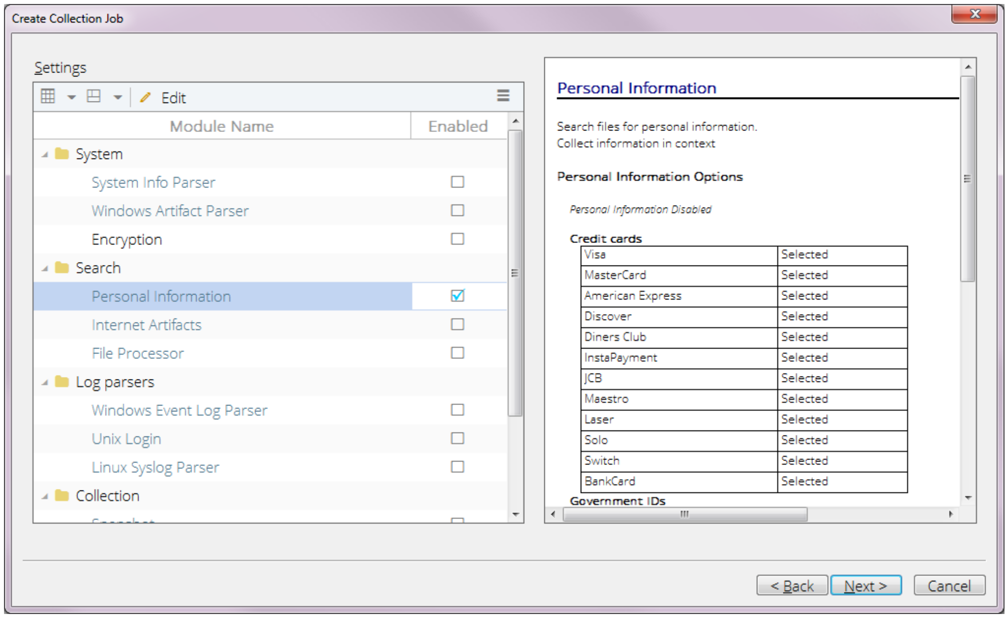
Modules are used to collect information about files and machines in specific ways. After naming a job, you select modules and configure them to your needs. To set module options, double click the module name. Most modules are collection modules that gather and collect information into an evidence (.Ex01/.E01) or logical evidence (.Lx01/.L01) file.

Some modules (such as the File Processor module) provide you with the ability to review and triage your information as it is being scanned on the target machine.

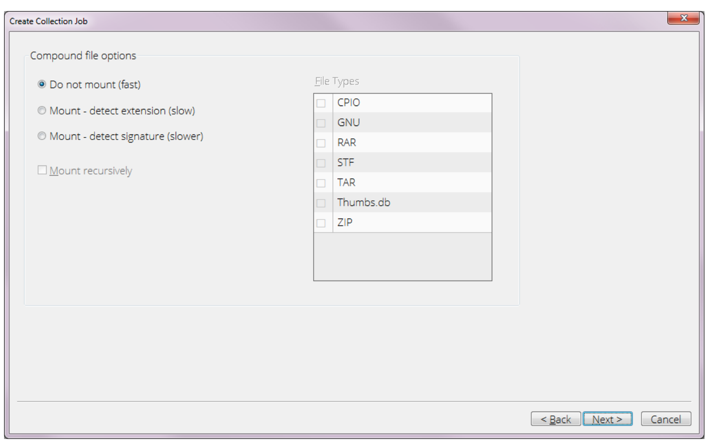
Creating a Portable Job

1. From the **Tools** dropdown menu open **Portable Management** or **Create Portable Device**, or from the EnScript dropdown menu open **Portable Management**.
2. In Portable Management, click **New** in the Select Jobs area; from within EnCase Portable, click **New** in the EnCase Portable dialog. The Create Collection Job dialog displays.
3. Rename or accept the default text in the Job name field.
   - The default job name is `Job__[yyyy_mm_dd__hh_mm_ss]`, using the current date and time of your local system. Example: Job___2017_02_14__03_42_42_PM
   - A job name cannot contain spaces at the beginning or end of the name, or any of the following characters: `\ / : * ? " < > |`
4. Text entered in the Description field (optional) is aligned with job names under Recent Jobs in the Portable Home screen.

5. Click **Next** to open the Module Selection dialog. This dialog shows module groupings in the left pane and the current configuration options for the selected module in the right pane.



6. Select one or more modules by checking the checkbox by the module's name.
7. When available, options for each module can be selected by double clicking the module name. For more information, see documentation for the specific module.
8. Click **Next** to open the Compound File Options dialog.



The Compound File Options dialog provides options for whether compound file types selected in the File Types box are mounted (unpacked) and scanned.

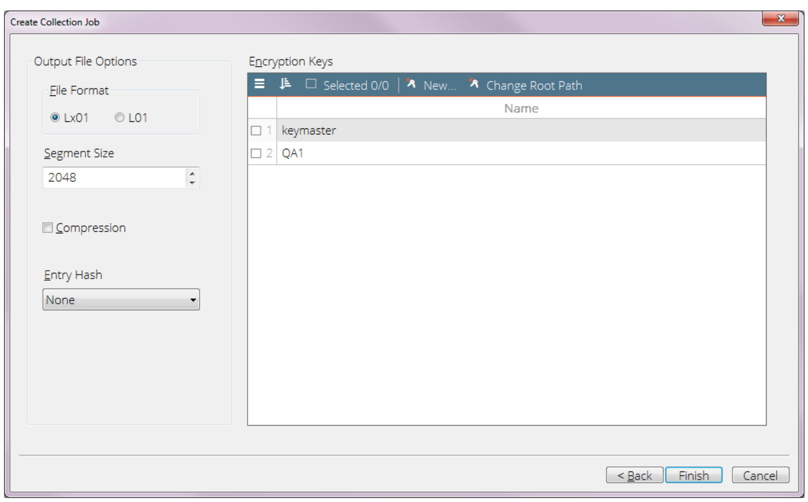
If any option other than the first option is selected, you can select how to detect which files to mount and select the specific file types to process:

- **Do not mount** does not perform any unpacking of compound files, so the files are processed without unpacking any of the internal content.
- **Mount - detect extension** causes files with a matching extension to be mounted and processed. No signature verification is conducted.
- **Mount - detect signature** results in a signature analysis being run on all files to determine if they are a compound file of interest. Files with the correct signature are then mounted and processed.

If you choose to mount files, you are given further options:

- **Mount recursively** mounts any compound files found inside a compound file.
- The **File Types** checkboxes let you select which of the supported compound file types to process.

9. Click **Next** to open the Output File Options dialog. This dialog provides control over the format of the collected evidence.



- **File Format** options determine the type of file to create. Lx01 format is an encrypted logical evidence files. L01 format is a legacy unencrypted logical evidence file.
- **Segment Size** determines the size, in megabytes, of the individual segments of the evidence file.
- Check **Compression** to compress the size of the EnCase evidence file.
- Use the **Entry Hash** dropdown to select the type of hash algorithm used for each file system entry.
- The **Encryption Keys** box enables you to add multiple encryption keys for use in encrypting Lx01 files. Evidence collected when triage is enabled cannot be

encrypted.

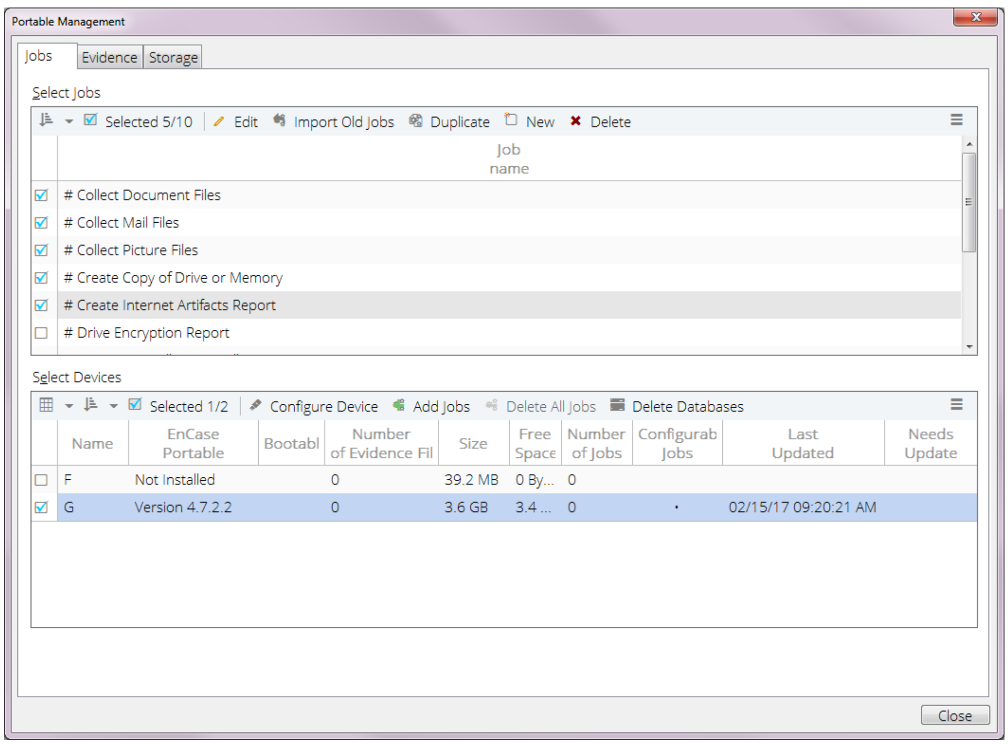
– **New** allows you to generate a new encryption key.
– **Change Root Path** enables you to specify a folder where EnCase encryption keys are stored.

10. Click **Finish** to create the job.

Adding a Job to the Portable Device

If you have created a collection job in EnCase, you must add it to the Portable device to execute.

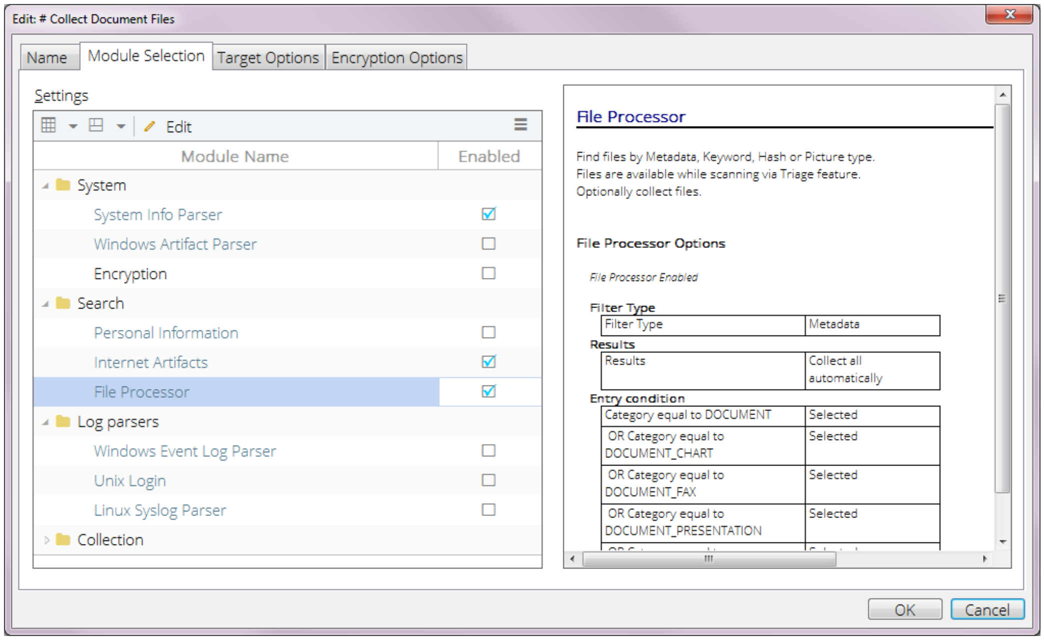
1. Select **Tools** > **Portable Management**.



2. In the Select Jobs table, select the jobs you want to add to the Portable device.
3. In the Select Devices table, select the device you want to add the jobs to.
4. Click **Add Jobs**. The Adding Jobs status window displays the updating process.
5. When completed, click **Finished**.

Modifying a Job

1. Select **Tools** > **Portable Management** and double click the job you want to modify. The Edit: # Collect Document Files dialog displays.



2. The tabs display the previously selected settings. Modify the name, module selections, module options, target options, and encryption options as desired and click **OK**.

Duplicating a Job

1. Select **Tools** > **Portable Management**.
2. Select the job to duplicate in the **Select Jobs** section and click **Duplicate**. The Copy Job dialog displays.
3. Enter a new name for the job and click **OK**. EnCase transfers all the settings from the first job to the new job.
4. Edit the new job to modify its settings.

Finding Jobs

By default, jobs are stored on the Portable device in the `\Jobs` folder. Using Windows Explorer, or another file management tool, copy or move the .enjob file to the desired location on your local drive or other device.

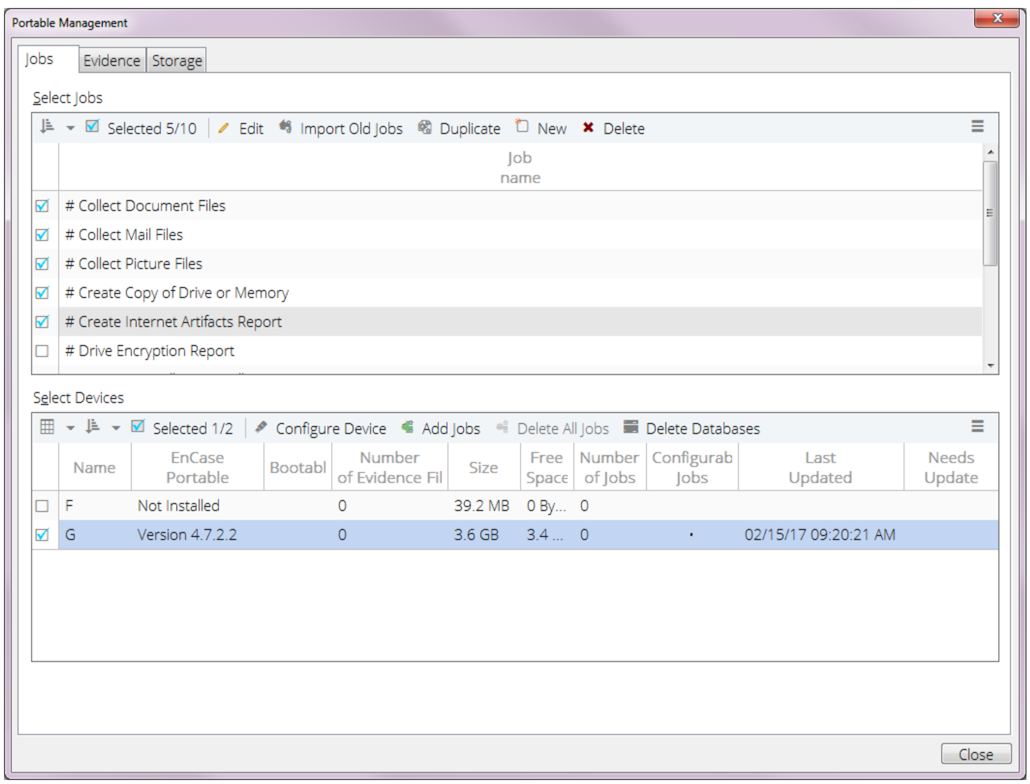
If a job is not contained in the `\Jobs` folder you can find its location by finding and opening its containing folder:

1. Select **Tools** > **Portable Management**. The Portable Management dialog displays.
2. In the Select Jobs section, right click the job name you want to locate and select **Open Containing Folder**.
3. A dialog displays the location of the file in the folder hierarchy.
4. By default, user-created jobs are stored in the `\Documents\EnCase\Storage` folder created in the user profile folders of your EnCase installation. If you are using the standalone version of Portable, user-created jobs are stored in the `\Jobs` folder on the Portable device.

Updating Older Jobs

You can import .ini jobs created in older versions of Portable to make them into .enjob jobs compatible with the current version.

1. Select **Tools** > **Portable Management**. The Portable Management dialog displays.



2. In the Select Jobs section of the Jobs tab, click **Import Old Jobs**. The Browse For Folder dialog displays. Navigate to the version of EnCase you are currently running.
3. Select the specific storage location of the jobs and click **OK**. The Importing Old Jobs dialog displays.

4. All .ini jobs are converted to the new .enjob format. When done, click **Finished**. The imported jobs are displayed in Portable Management.

Deleting Jobs

DELETING A JOB USING PORTABLE MANAGEMENT

1. From the Portable Management **Jobs** tab, select a job to delete.
2. Click **Delete**. A confirmation dialog displays.
3. Click **OK** to delete the job.

DELETING A JOB FROM PORTABLE

1. From the Portable home screen, select the **Configure Jobs** option.
2. Portable displays the Configure dialog.
3. Select a job or jobs to delete by checking checkboxes and click **OK**. A confirmation dialog displays.
4. Click **OK** to delete the job.
5. If no jobs are selected, the **Delete** button on the toolbar, or the **Delete** option on the right click menu, deletes the currently highlighted job after confirming the deletion with the user. The **Delete All Selected** right click menu option is disabled.
6. If at least one job is selected by clicking its checkbox, the **Delete** button on the toolbar deletes the checked job, as will the **Delete All Selected** right click menu item.

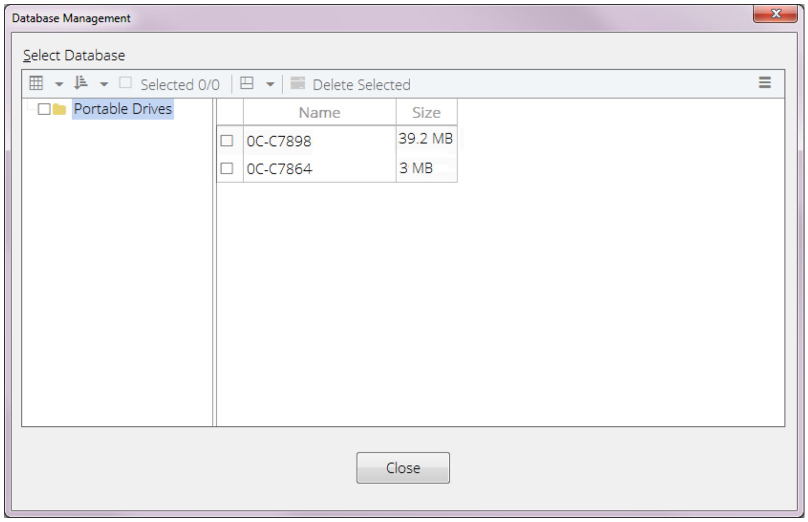
Note: Any jobs that are currently running are not deleted.

Deleting All Jobs from the Portable Device

1. Select **Tools** > **Portable Management** and select the device(s) to delete jobs from.
2. Click **Delete All Jobs**. EnCase Portable deletes all jobs on the selected devices.

Deleting Target Databases from the EnCase Portable Device

1. Select **Tools** > **Portable Management**. The Portable Management screen displays, with the **Jobs** tab selected.
2. In the **Select Devices** section, select a device. The **Delete Databases** button becomes enabled.
3. Click **Delete Databases**. The Database Management dialog displays.



- All portable devices that hold at least one target database are displayed, along with all target databases present on each device.
- Clicking the device name in the left pane automatically selects all target databases present on that device.
- After selecting at least one target database, the **Delete Selected** button becomes enabled.

4. Select all target databases you want to delete.
5. Click **Delete Selected**. All selected target databases are deleted and the dialog refreshes to show the remaining databases.
6. When done, click **Close**.

System Modules

System modules collect information about files and machines. Most of these modules contain options that you can configure for your specific needs. To set module options, double click the module name.

Most modules are collection modules that gather and collect information into an evidence (.Ex01/.E01) or logical evidence (.Lx01/.L01) file.

Some modules (such as the File Processor module) let you review and triage your information as it is being scanned on the target machine.

System Info Parser

The System Info Parser module obtains information about the target machine, including its operating system, installed software, hardware components, network configurations, mapped drives and shares, and so forth.

The module works with both Linux and Windows operating systems, and displays different data depending on the operating system of the collection target. The module also uses different files to parse the data, depending on the system. For Windows systems, all data is collected from the Windows registry. For Linux systems, the data is compiled from various configuration files found throughout the file system.

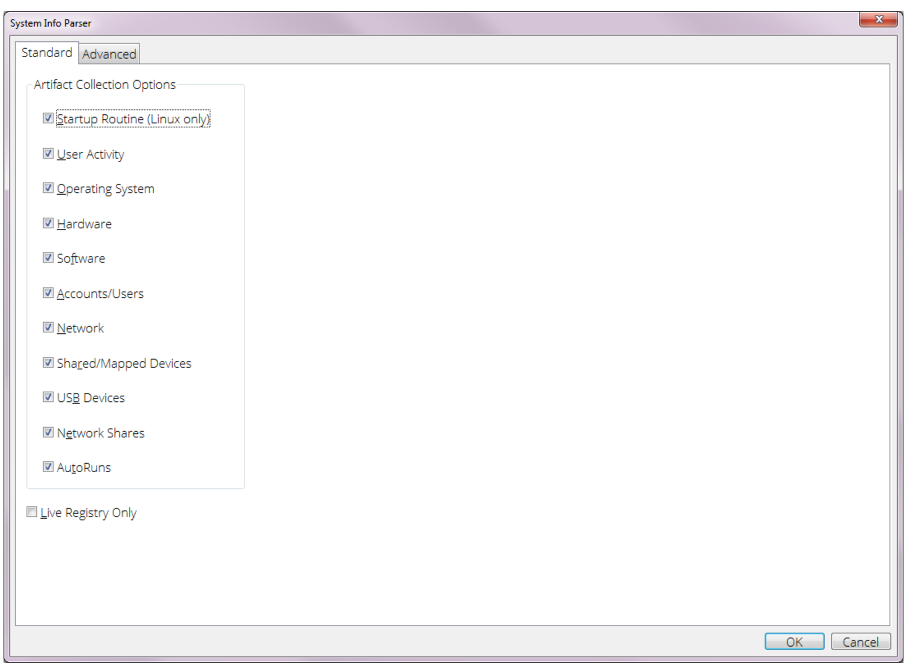
The following Linux systems are supported:

- Ubuntu 8
- Fedora 8

The job summary displays results based on the options selected from the **Standard** and **Advanced** tabs.

STANDARD OPTIONS

The **Standard** tab of the System Info Parser lets you choose from categories of data that can be collected. These categories correspond to different data stores on the target machines, depending on the operating system.



The following options can be set in the **Standard** tab:

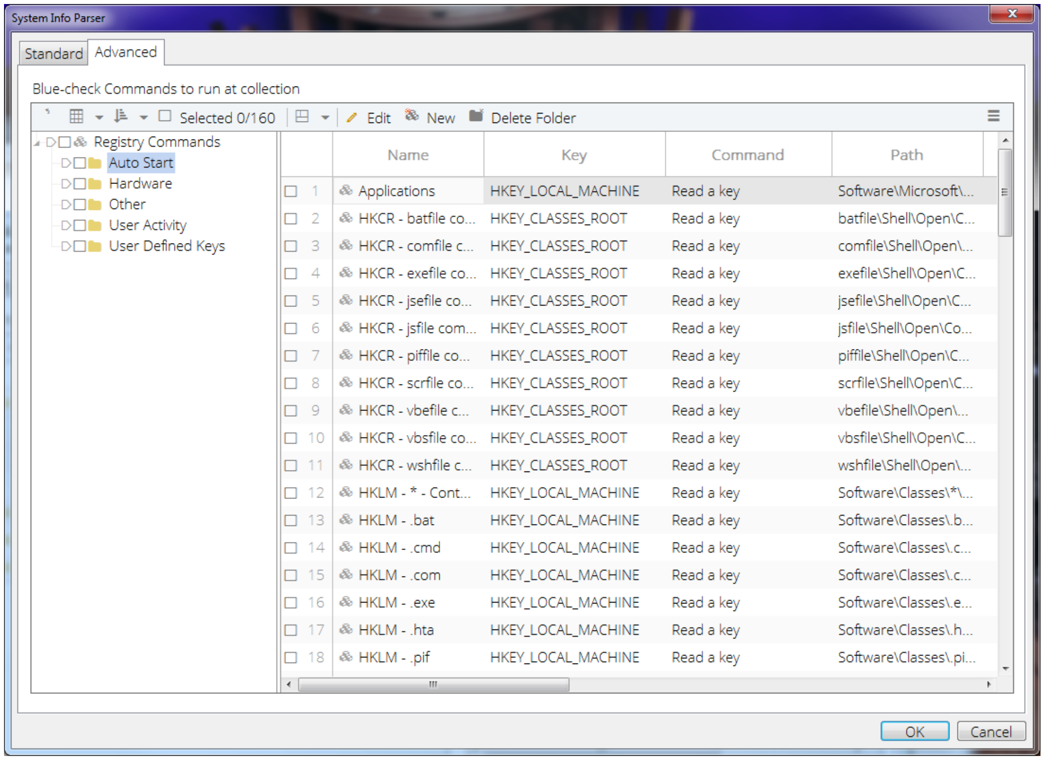
- **Startup Routine** (Linux only) retrieves information from supported Linux systems about scripts that execute when the system starts and shuts down.
- **User Activity** (Linux only) retrieves information from supported Linux systems pertaining to typed user commands. This information depends on what shell is being used.
- **Operating System** retrieves:
  - The time zone of the computer.
  - System startup mode information, such as the default place to save startup scripts.
  - Login prompt and version information shown during startup.
  - Boot manager information.
  - Language settings.

- **Hardware** retrieves the hardware configuration of the computer as it was checked during startup, including hardware adapters/devices, architecture information, and so forth.
- **Software** retrieves two types of software information:
  - Cron jobs scheduled to run at particular times.
  - All applications installed on the computer.

- **Accounts/Users** retrieves user and password information, including domain users who have logged onto the machine.
- **Network** retrieves information about interfaces and their corresponding device names and options, as well as the host name of the computer.
- **Shared/Mapped Devices** retrieves information about mapped or mounted network shares and drives.
- **USB Devices** retrieves history of USB device use from the Registry.
- **Network Shares** retrieves "shellbag" keys which record what UNC paths a user visits.

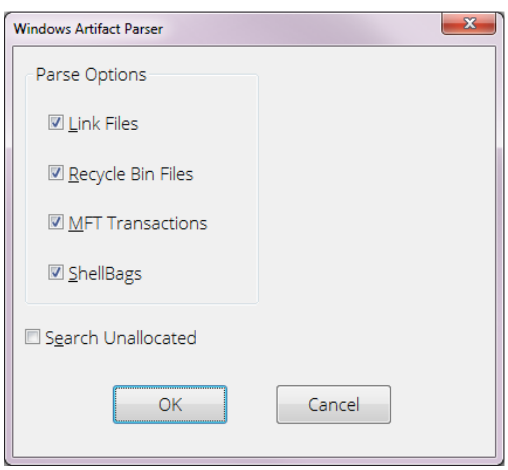
ADVANCED OPTIONS

The **Advanced** tab lets you specify registry keys to collect from target machines running Windows. You need to know the Windows version-specific locations of relevant data within the registry before using this tab.



Windows Artifact Parser

The Windows Artifact Parser module searches for information in link files, recycled files, Master File Table transaction logs, and shellbag artifacts.



Windows Artifact Parser module includes three options:

- **Link Files** creates an output artifact for each Link file (usually *.lnk) found during preprocessing. This selection adds Created, Accessed and Modified data properties plus

the path to the file that is referenced by the link to each output artifact.

- **Recycle Bin Files** creates an output artifact for each item found in the file that holds information about deleted files. This selection adds the path of the original file location as the path data property to each output artifact.
- **MFT Transactions** creates an output artifact for each item in the Master File Table transaction log "$Log" file (which records all redo and undo information for each user file that is updated). This selection adds Created, Written, Accessed, and Modified data properties to each output artifact for these types of items.
- **ShellBags** creates an output artifact for registry keys that indicate size, view, icon and folder position used within Windows Explorer.

Select **Search Unallocated** to enable a search of unallocated space for the Windows Artifacts.

Encryption

The Encryption module produces a single page report listing the encryption type of each drive and volume on the target system. After jobs using this module are run, the report is available as a Summary Report and as the Encryption Report in standard reports.

This module is used only on machines that are already running, and depends on core encryption analysis. It does not work on evidence files.

Only supported encryption types are shown; do not assume that a device is not encrypted if its encryption type is not displayed.

This module has no configurable options.

Search Modules

Search modules to find information about files and machines in specific ways. Most of these modules contain options that you can configure. To set module options, double click the module name.

Personal Information

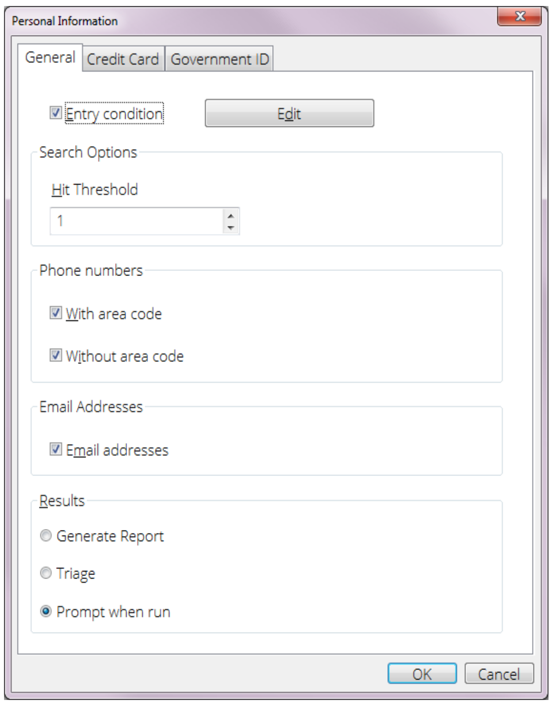
The Personal Information module collects information about files containing personal information. By default, this module searches all document, database, and Internet files and identifies files containing the types of personal information listed below. Files are identified but the information and the file itself are not collected. Reports show which files have personal information content, and what type of content that is. This prevents potential abuse of this kind of data.

Jobs created with the Personal Information module let you triage the scanned data as it is being gathered. You can stop a scan when you find the information you are seeking or determine that the scan will not prove useful.

For more information, including the GREP expressions used, see FAQs on page 381.

The following options can be set in this module:

GENERAL TAB



Select **Entry condition** and click **Edit** to specify or modify which conditions are used to search for the personal information selected. By default, the entry condition is set to search only files that match the document, database, Internet, or unknown file categories.

The **Hit Threshold** lets you ignore files with only a few hits. For example, if you set the threshold to 5, only files containing five or more PII hits are collected. Any file with fewer than five hits is ignored. The default is 1.

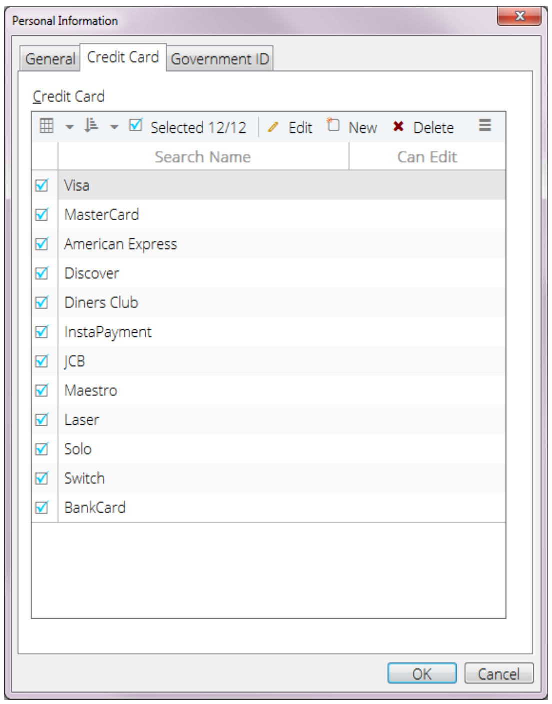
The **Phone numbers** options find information containing U.S. and Canadian formatted phone numbers, with or without separators. You can select whether to search for numbers with or without area codes.

Select **Email addresses** to identify email addresses.

The results section enables you to choose how you want to receive the results of your search:

- **Generate Report** allows jobs to run normally without triaging data as it is being collected.
- **Triage** displays data for review by the examiner, as it is being collected.
- **Prompt when run** lets you turn the Triage feature on or off during data acquisition.

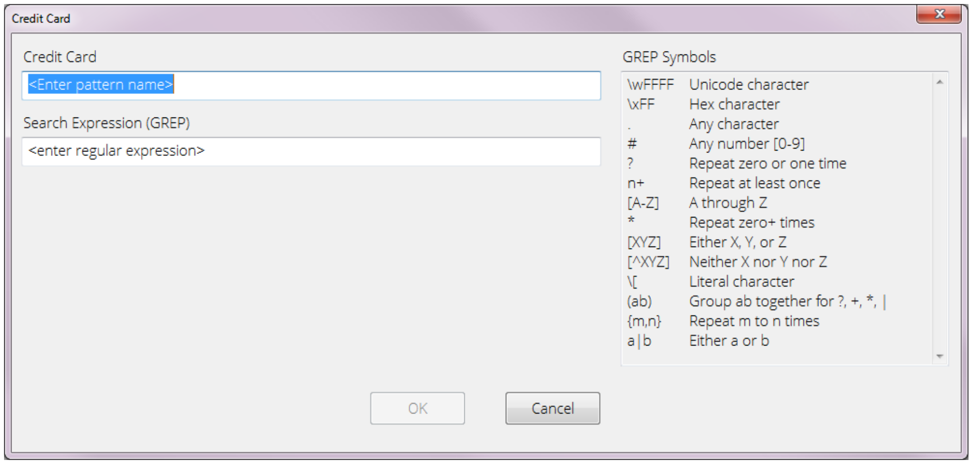
CREDIT CARD TAB



Pre-configured options are provided to identify major credit card numbers.

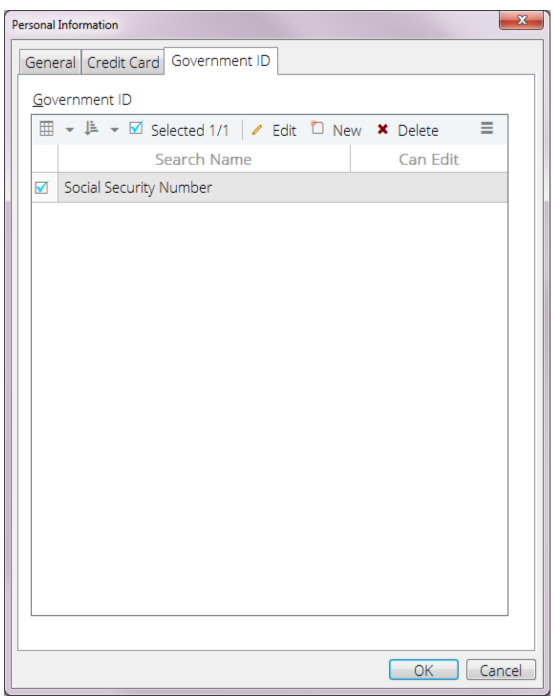
- All detected numbers are subjected to validation to prevent random 16-digit numbers from being identified.
- Credit card number validation is performed using the Luhn or Modulus/Mod 10 algorithm.
- Both card numbers with separators (1234-5678-9012) and without separators (123456789012) are identified.

You can customize a credit card search by clicking **New**. The Credit Card Data dialog displays:



- Customized credit cards are signified by a dot in the Can Edit column.
- Click **Edit** to modify a customized credit card.
- Click **Delete** to remove a customized credit card.
- Results are validated with the Luhn algorithm.

GOVERNMENT ID



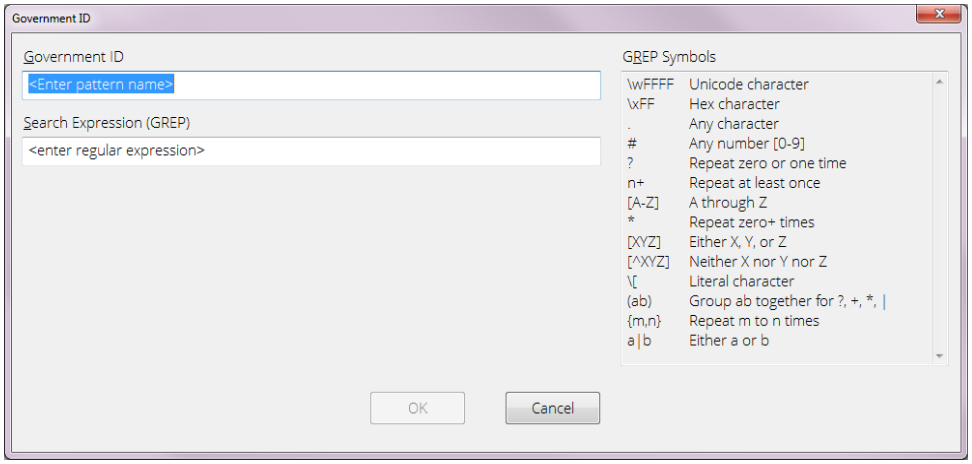
The Government ID tab enables you to search for any type of government ID (not just Social Security numbers) through the use of GREP expressions. This is especially useful in areas where government issued IDs have different formats.

The hits are indexed and searchable using the Government ID pattern query.

Social security numbers finds U.S. social security numbers, with or without separators.

> **Note:** You cannot view or edit the default Social Security Number.

To add another type of ID, click **New**. The Government ID dialog displays.



- Enter a name in the **Government ID** box and a GREP expression in the **Search Expression (GREP)** box.
- When done, click **OK**.

Internet Artifacts

The Internet Artifacts module collects and analyzes Internet usage data from a target machine. The module assumes the target machine was used to access the Internet at least once.

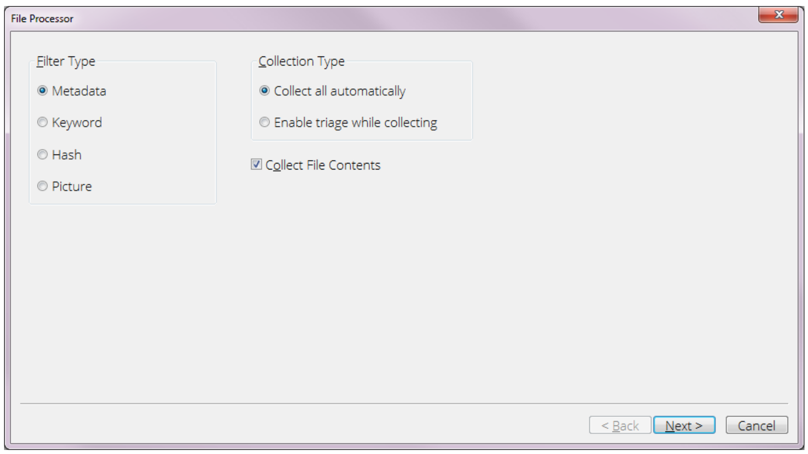
This module has no configurable options. Selecting the module captures the following information:

- **History** collects the user's browsing history.
- **Cache** collects cached information, such as the most recently requested web pages.
- **Cookies** collects stored cookie data.
- **Bookmarks** collects the user's bookmarks or favorite URLs.
- **Downloads** collects the data the user has downloaded from the Internet.

File Processor

The File Processor module is a multipurpose module that enables you to select from four types of file processing, then choose how you want to handle the final results.

The File Processor module provides you with the option to view evidence as it is being collected. You can stop a scan when you find the information you are seeking or determine that the scan will not prove useful.



The four filter types available in the File Processor module include:

- **Metadata** processing specifies the types of files to be searched for, using a set of entry conditions. See Metadata on the next page.
- **Keyword** provides a way to find information based on a list of entered keywords, and lets you refine the search with an entry condition. This option allows GREP expressions, whole word, and case sensitive searching. See Keyword on page 345.
- **Hash** searches for files by comparing their hash values to hash values found in either a new or pre-existing hash set. This option lets you create a new hash set or use a pre-existing set, and also lets you refine the search with an entry condition. See Hash on page 347.
- **Picture** searches for files identified with a file category of "picture." This option lets you limit the number of files that are returned, and limit the minimum size of the pictures. In addition, you can add entry conditions to further refine your search. See Picture on page 348.

The results of your processing can be handled in two ways:

- **Collect all automatically** collects everything that is responsive and creates an evidence file for further analysis. When you select this option, jobs that include this module automatically complete the collection and save it as an evidence file.

- **Enable triage while collecting** lets you review the evidence as it is being collected. This lets you triage the information as it is being gathered. You can then review your information in real time, specifically select the information you want to examine further, and save that information as a logical evidence file (LEF).
- **Collect File Contents** copies the contents of files identified by the file processor into the logical evidence file (LEF).

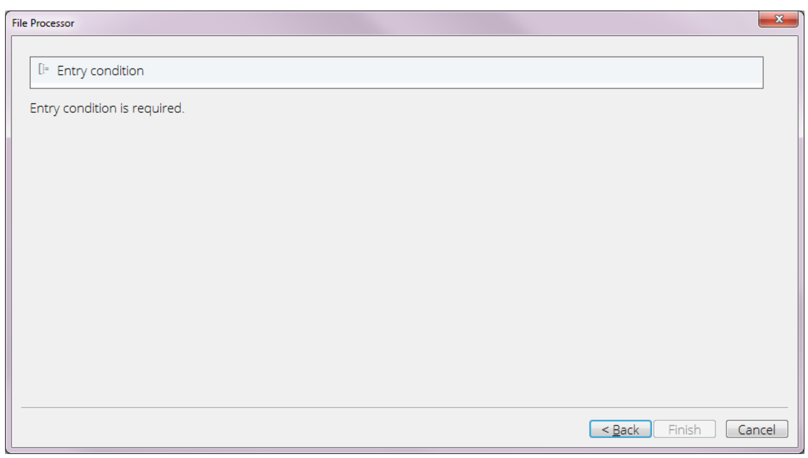
To configure the File Processor module, select one of the processing types, and choose one of the ways to handle the results.

Click **Next** to display the options screen for the processing type selected.

METADATA

The File Processor module **Metadata** processing option collects specific types of files using entry conditions. For example, you can set it to collect all types of images (.jpg, .png, .bmp, etc.) or documents (.doc, .xls, .pdf, etc).

Click on **Entry condition** to create or edit entry conditions. Set conditions to specify exactly which files your job collects. The default metadata condition will target all files if left unmodified.



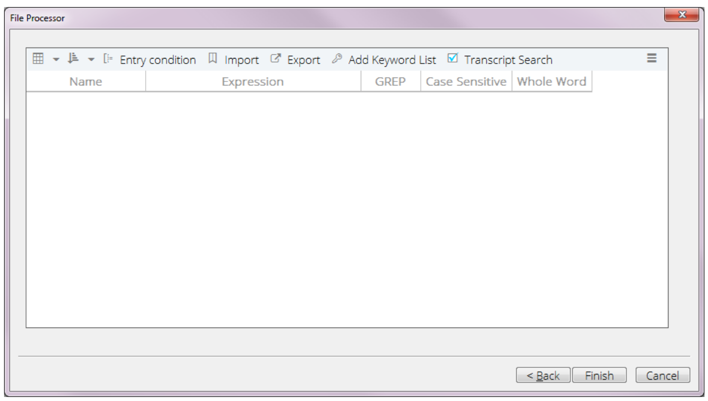
After setting entry options, click **Finish**.

KEYWORD

The File Processor module **Keyword finder** processing option lets you create a list of keywords for searching documents on a target machine. The Keyword finder module contains an Entry Condition which targets searchable documents. See the Customization section for instructions on viewing and modifying default conditions.

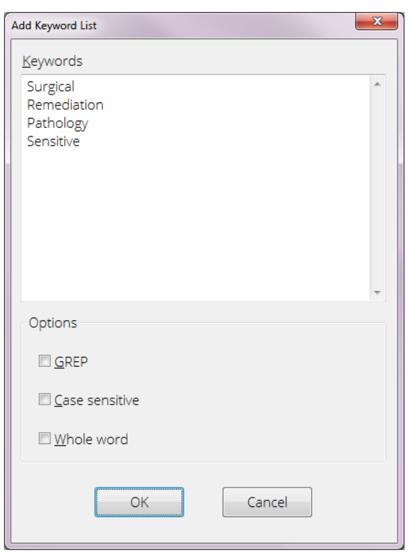
> **Note:** This module searches the transcript of files supported by Oracle Outside In viewer technology. This differs from the keyword searching in EnCase in that this method locates keyword hits inside of files (such as .docx or .xlsx files) that would not be found by a raw search of the file.

After clicking **Next** in the File Processor module, the Keyword options dialog displays:



ADDING A LIST OF KEYWORDS

To compile a list of keywords, click **Add Keyword List**. The Add Keyword List dialog displays.



1. Add the keywords to the text box, one per line.
2. Select the appropriate checkbox option if the keywords should be interpreted as GREP expressions, case sensitivity should be enforced, lines should be treated as whole words.
3. Click **OK**.

IMPORTING KEYWORDS

To import a list of keywords that has been exported from EnCase, click **Import**. The Import Keywords dialog displays.

Browse to the keywords file location, select a file, and click **OK**.

EDITING KEYWORDS

To edit a keyword in the Keyword Finder, select it in the options dialog and click **Edit**. The Edit Keywords dialog displays:

1. Edit the keyword name or expression.
2. Change keyword options, if needed.
3. Click **OK**.

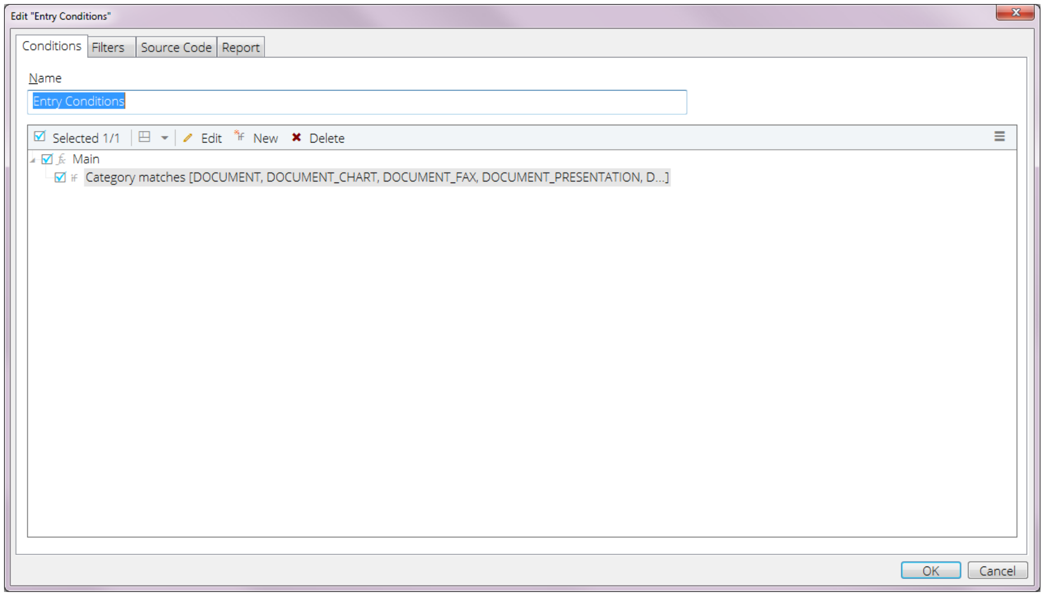
EXPORTING KEYWORDS

To export the list of compiled keywords, click **Export** on the Keyword Finder dialog. The Export Keywords dialog displays.

Enter a new filename and click **OK**. This keyword file can be used in EnCase.

CUSTOMIZATION

To specify which files the Keyword processes, click **Entry Condition** in the Keyword options dialog to open a conditions dialog. By default, the entry condition restricts processing to files where the category matches "Document."



After setting your options, click **Finish**.

HASH

The **Hash** processing option in the File Processor module searches for files with a particular hash value on the target machine. Hash values are stored in hash sets that can be identified by a name and category. The Hash Finder module targets all files by default. You can customize these default conditions.

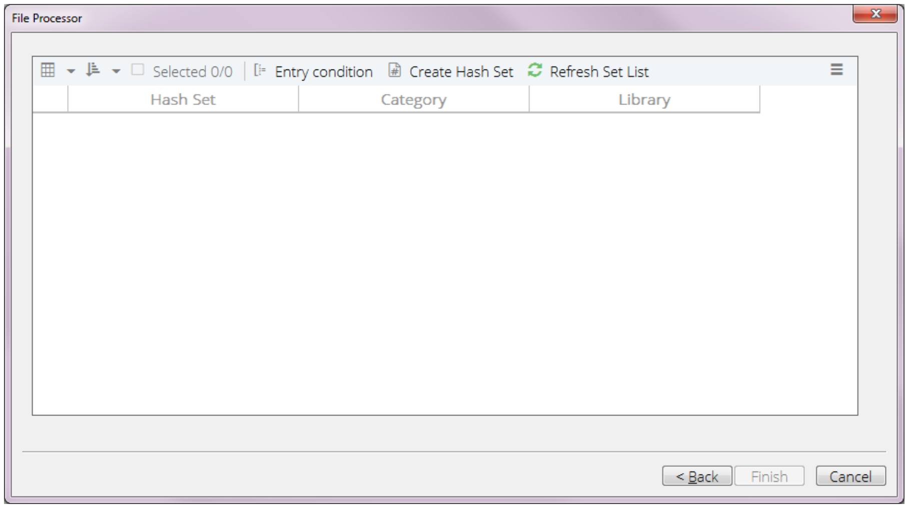
Before you can use the **Hash** processing option, you must create hash sets for your current case.

Hash sets can be added to the module from the following sources:

- A hash set created from a folder. When created this way, you can assign a name and category to assign to the set.
- A hash .bin library available in EnCase:
  - Existing .bin library files have a category if one was specified.
  - The name of the hash set is the name of the .bin library file.

When the **Hash** processing option is used in a job, the hash sets are kept in their original location and also copied to the EnCase Portable USB device.

After clicking **Next** in the File Processor module, the Hash options dialog displays.



The hash sets displayed, if any, are taken from the hash library. You can select from an existing hash set in this list, or create a new set. Click **Refresh Set List** to add all other available hash sets to the list.

CREATING A HASH SET

To compile a hash set, click **Create Hash Set**. The Create Hash Sets From Folder dialog displays.

- Enter or browse to the folder containing the files you want to create a hash set from.
- The Hash set name is automatically populated using the name of the folder. You can change the hash set name.
- Enter a category for this hash set (optional).
- Click **OK**. EnCase creates a .bin library file from the files in the selected folder, saves it to the EnCase Hash Sets folder, and adds it to the Hash Finder options list.

CUSTOMIZATION

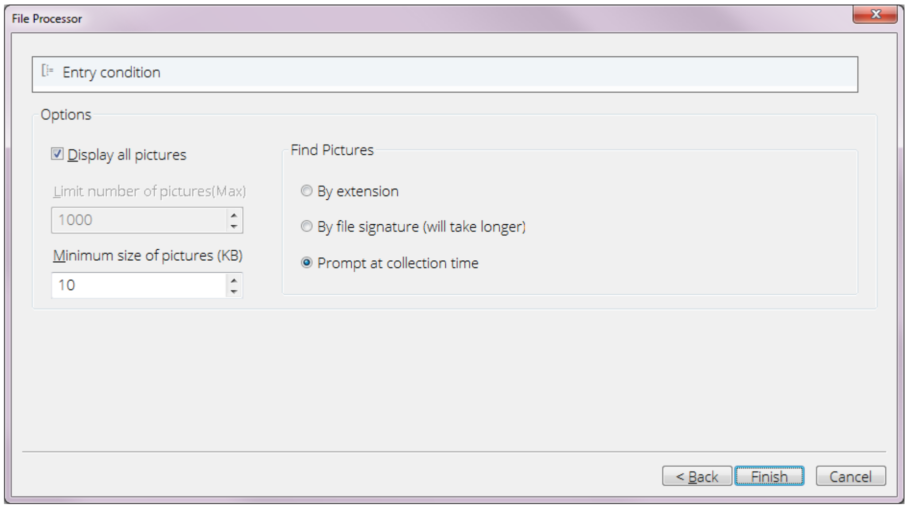
To further specify your results, click **Entry Condition** to open up a conditions dialog.

After setting all options, click **Finish**.

PICTURE

Use the **Picture** processing option in the File Processor module to search for pictures on a target machine. This module contains an Entry condition which returns files that match the picture file category in EnCase. See the Customization section for instructions on viewing and modifying default conditions.

After clicking **Next** in the File Processor module, the following dialog displays:



- To limit the number of pictures returned, clear the **Display all pictures** checkbox and adjust the number in the **Limit number of pictures** option.
- The default is set to gather all pictures above 10KB in size. If you want to change the minimum size of the picture files returned, adjust the **Minimum size of pictures** option.
- You can select to find pictures either by file extension or by file signature.
  - **By extension** finds all files by category, as determined by the file extension (for example, .jpg, .bmp, or .png).
  - When you select **By file signature**, EnCase Portable checks the file signature of an entry to see if it is a picture. This collects pictures that have been renamed by changing their file extensions.
  - **Prompt at collection time** displays a dialog when you are running the job, which lets you search by file extension or by file signature.

After setting your options, click **Finish**.

CUSTOMIZATION

To specify which files the Picture Finder processes, click **Entry condition** in the Picture Finder options dialog to open a conditions dialog.

The Picture Finder module only returns files that match the file category of "picture" in EnCase. Although additional options can be specified in the entry condition, this particular parameter cannot be modified.

Log Parser Modules

Log parser modules parse and collect information from Windows event logs, Unix login files, and Linux login and system files.

Windows Event Log Parser

The Windows Event Log Parser module parses and collects information pertaining to Windows events logged into system logs, including application, system, and security logs. The module parses .evt and .evtx files for Windows Event Logs, and also allows for processing by condition.

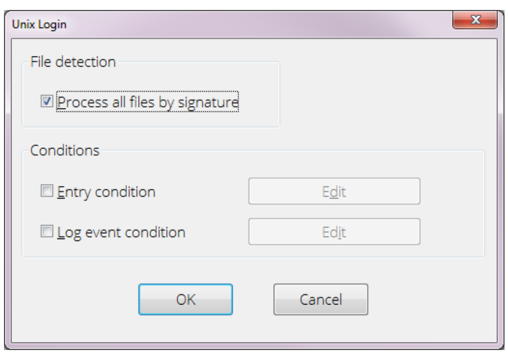
Conditions restrict which files to look at and what entries to parse.

- **Entry condition** filters which files EnCase processes, based on their entry properties.
- **EVT condition** restricts individual events on properties parsed from an EVT file (Event ID, Event Type, Source, etc.).
- **EVTX condition** restricts individual events on properties parsed from an EVTX file (Event ID, Process ID, Thread ID, etc.).

To enable a condition, select its checkbox. Click Edit next to the condition type to modify the condition.

Unix Login

The Unix Login module parses the Unix system WTMP and UTMP files, which record all login activities. In the module analysis reports, the WTMP-UTMP Log Parser provides information about machines, login types, and login messages.



File detection determines how the module detects authentic event files. By default, file detection is performed by looking for event files with a proper extension, then verifying their signature to prevent processing incorrect files. When checked, **Process all files by signature** causes the module to determine event files based on their file signature only. Check this box to detect event file logs that contain an incorrect extension.

Conditions restrict which files to look at and what entries to parse.

- **Entry condition** restricts which log files EnCase processes.
- **Log event condition** determines which entries from the processed log files are examined. If a condition is applied, EnCase collects only those log entries that meet the condition.

To enable an entry condition, select its checkbox. Click **Edit** next to the conditions selected, to modify the conditions that determine which files are processed.

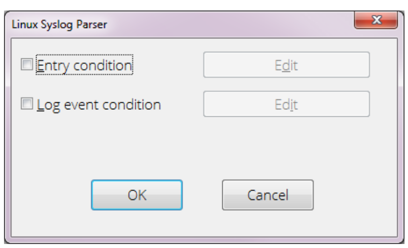
Linux Syslog Parser

The Linux Syslog Parser module collects and parses Linux system log files and their system messages for Apple Macintosh and Linux machines. It then is able to provide information about the machine, log file summaries, and log messages.

On a Linux target, the `\etc\syslog.conf` file is parsed for paths that contain the system log files.

On an Apple Macintosh target, the `\private\etc\syslog.conf` file is parsed for the paths that contain the system long files.

Click **Edit** to modify the conditions that determine which event parameters are collected.



- Use **Entry condition** to create a condition that restricts which Linux syslog files are processed.
- Use **Log event condition** to specify syslog conditions that can filter by host name, process, message, and so on.

To enable an entry condition, select its checkbox. Click **Edit** next to the conditions selected to modify the conditions that determine which files are processed.

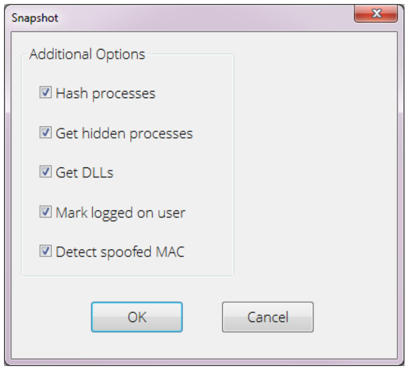
Collection Modules

EnCase Portable uses two collection modules to collect information about files and machines in specific ways.

- The Snapshot module takes a snapshot of a machine at a given time.
- The Acquisition module acquires images of drives and memory from a target machine.

Snapshot

The Snapshot module collects a snapshot of a machine at a given time, including the running processes, open ports, network cards, login information, open files, and user information.

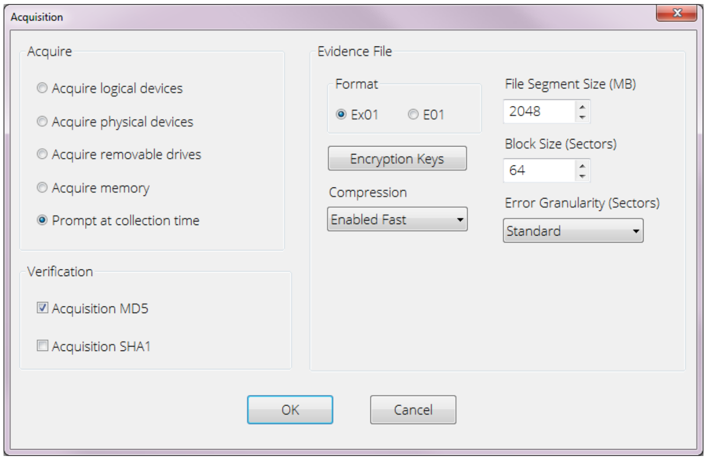


Snapshot module options:

- **Hash processes** calculates hash values for the executable files that were run to create the currently running processes.
- **Get hidden processes** identifies processes that have been hidden from the operating system.
- **Get DLLs** retrieves and collects a list of currently loaded DLLs.
- **Mark logged on user** finds and marks which of the identified users are currently logged on.
- **Detect spoofed MAC** detects if the MAC address for any of the network interfaces is being set to a value other than the default value.

Acquisition

The Acquisition module acquires images of drives and memory from a target machine. When using this module, ensure you have enough storage available to hold the evidence files this process creates.



Acquisition module options:

ACQUIRE

- **Acquire logical devices** acquires all logical devices (lettered drives, such as C:).
- **Acquire physical devices** acquires all physical devices (numbered devices, such as 0, 1, etc.).
- **Acquire removable drives** acquires all removable drives. A drive is identified as removable by the operating system.
- **Acquire memory** acquires an image of machine memory (RAM).
- **Prompt at collection time** displays a list of all devices (logical, physical, and memory) when the job is run. Select any combination of these devices for acquisition.

> **Note:** To automatically acquire more than one type of device, create separate jobs for each operation. Because EnCase runs in memory, Guidance Software suggests you capture memory first.

EVIDENCE FILE

- **Format** options determine the type of file to create.
  - **Ex01** files are encrypted full disk acquisition files.
  - **E01** files are unencrypted full disk acquisition files.

- **File segment size (MB)** determines the size, in megabytes, of the individual segments of the evidence file.
- Click **Encryption Keys** to open a dialog that enables you to add multiple encryption keys for use in encrypting Ex01 files.
  - **New** allows you to generate a new encryption key.
  - **Change Root Path** enables you to specify a folder where EnCase encryption keys are stored.

- **Block size (sectors)** determines the block size of the contents where CRC values are computed.
  - The minimum value is 64 sectors.
  - Larger block sizes generally enable faster acquisitions. However, if an evidence file block becomes damaged, a larger amount of data will be lost.

- Use the **Compression** dropdown menu to determine whether to enable or disable the compression of evidence files.
  - **Disabled** does not compress evidence files.
  - **Enabled** compresses evidence file size.

- **Error granularity (sectors)** determines how much of the block is zeroed out if an error is encountered.
  - **Standard** is the same value as the block size.
  - **Exhaustive** sets granularity to one sector. This retains more data but takes more time.

VERIFICATION

- **Acquisition MD5** calculates the MD5 file hash of the acquired files.
- **Acquisition SHA1** calculates the SHA-1 file hash of the acquired files.

VERIFYING ACQUIRED EVIDENCE

When running a collection job using Acquisition module, EnCase can verify the acquired files using hash values.

Before the job runs, a dialog displays listing the storage path, available drives, and a **Verify acquisition** checkbox.

Check the **Verify acquisition** checkbox to verify the hash values of the acquired evidence files. This adds time to the running of the job.

When completed, EnCase includes both the original and the verification hash values in analysis tables and reports.

Screen Capture

The Screen Capture module preserves images of each open window on a running machine. Images are saved in a logical evidence file.

The contents of minimized windows may not be able to be gathered.

This module has no configurable options.

Collecting Evidence

This section describes how to:

- Run jobs.
- View information as it is being collected.
- If EnCase is installed, copy evidence into EnCase from a Portable storage device.

Before you begin, you will need:

- A correctly configured Portable device. See Installation and Configuration in the EnCase Portable User's Guide.
- The jobs to be exported to the Portable device (see Creating a Portable Job on page 327 and Adding a Job to the Portable Device on page 330).
- The correct configuration of storage devices, based on a knowledge of approximately how much data you are going to be collecting.

Running a Portable Job

You can run EnCase Portable on a running Microsoft Windows PC computer for which you have Local Administrator access. This method is not available for Apple Macintosh computers. Evidence cannot be acquired from floppy disks.

Before you begin, try to determine as accurately as possible how much evidence you will be collecting.

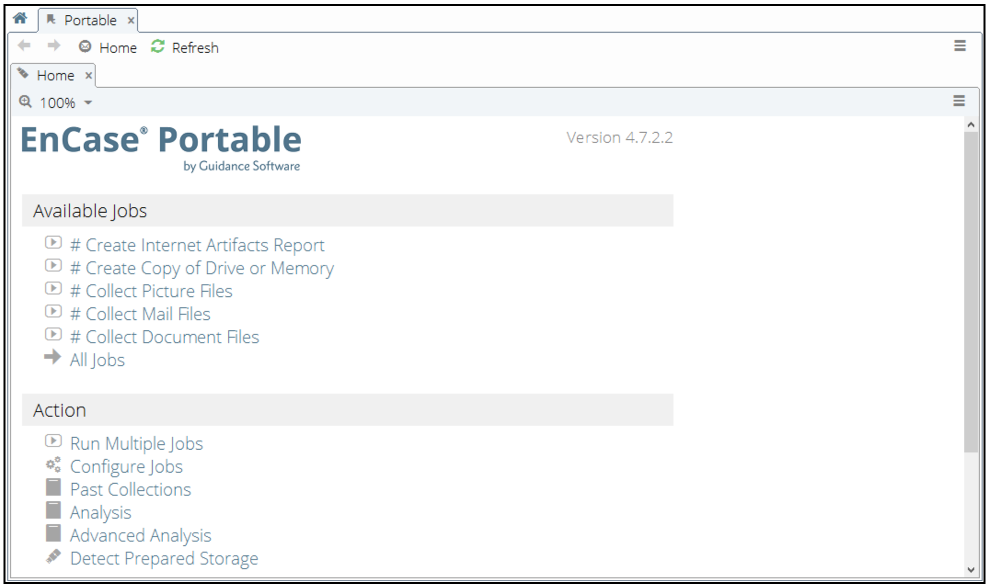
- If collecting less than 2.5 GB of data, use the Portable device to collect the evidence.
- If collecting more than 2.5 GB of data, use another prepared USB storage device to collect the evidence. If necessary, use the storage device with a USB hub.

To run a job on a target computer:

1. Insert a Portable device directly into a USB port.
2. If you are collecting more than 2.5 GB of data, plug the prepared Portable storage device into another USB port.
3. Navigate to the removable drive labeled EP-WIN and double click **Run Portable** to launch the application.
    - An optional quiet mode automatically installs the security key drivers, if needed, and launches without any more prompts. To run in quiet mode, note the drive let-

ter of the Portable device, then from a command prompt type <drive letter>`:\RunPortable.exe -q`.

4. The EnCase Portable screen displays.



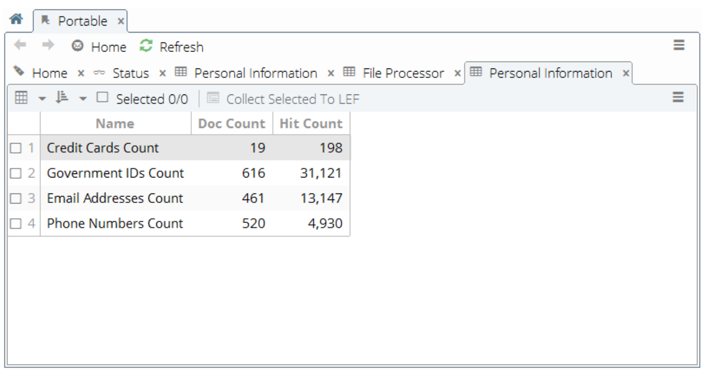
In the Configure Case section, the Case Name and Examiner Name are pre-populated, based on your case. You can edit them as desired. You can also optionally enter a description of the evidence.

5. Select a job to execute under Recent Jobs or click **Run Multiple Jobs** in the Action section.
6. You are prompted for additional information according to the job you selected. If you opted to **Run Multiple Jobs**, Portable displays the Select Job to Run dialog. A status dialog displays.
   - All modules used in the current job are listed.
   - When running a job using the File Processor module with triage results selected, EnCase updates the job status in real time while the job is executing. Clicking the status link displays the results as they are gathered. See Viewing Results to Triage Information on the facing page. At any point during the scanning process, click **Stop Scanning** to stop the job. This saves all data scanned to that point and terminates the job.
   - When running a job using the Acquisition module with the option selected to be prompted for acquisition choices when the job is run, a dialog displays showing a list

of devices to acquire. Selecting **Verify acquisition** causes the job to verify the hash values of the acquired evidence files. This increases the amount of time required to complete the job.

- When running a Picture Finder job using the File Processor module with the option selected to be prompted for how to find pictures when the job is run, a dialog displays asking whether to find pictures by extension or by file signature. Selecting to find pictures by file signature enables the collection of images that have been renamed with a different extension.

7. When a job is complete, or when you choose to stop scanning, a link to a summary displays in the Summary column for each module in the Status window. Click the link to open the summary.



- To create a report from selected items in the summary, select the items to include and click **Add Selected to Report**. See Creating a Report on page 366.

8. When done, close the status window.
9. To view the results of running your job, return to the Portable Home screen and select **Analysis** or **Advanced Analysis**.
10. When all jobs have completed, select **Exit** to close EnCase Portable.
11. After **Run Portable** closes, safely remove all EnCase Portable USB devices.

Viewing Results to Triage Information

When you create jobs using the File Processor or Personal Information modules, and select to triage the results, you can review your information as it is gathered. You can then stop a job as soon as you find the information you are seeking.

You can view results as they are gathered from:

- The File Processor module, which contains:
  - Metadata Entry Conditions
  - Keyword Finder
  - Hash Finder
  - Picture Finder
- The Personal Information module
- Any default job (such as # Triage Pictures) that enables triage

COLLECTING EVIDENCE

When you select to triage the results, you can review your information in real time, select the information you want to examine further, and save it as a logical evidence file (LEF). Blue check every document or file you want to save and then, when your job has stopped running, click **Collect Selected to LEF** from the job status screen. All selected items are collected and saved as a LEF. See Collecting Evidence from Triaged Results on page 364.

JOB ANALYSIS

After the job is completed, you can see this information again by clicking **Analysis** or **Advanced Analysis** in the Action section of the Portable home screen.

The **Analysis** or **Advanced Analysis** tab displays the available evidence.

Select **Collected Files** to view and review evidence.

Processing Files Using Metadata Entry Conditions

Metadata processing lets you identify potentially useful files using a set of metadata entry conditions, such as creating time, name of file, path, size, and so forth.

Options for metadata processing are configured when the job is created using the File Processor module.

While this type of file processing is running, you can view the progress screen by clicking the link in the status column of the status dialog. A list of files matching your entry conditions displays.

If the job has been configured to triage results, you can click any document name to view document files in the document viewer.

> **Note:** The document viewer does not work on non-document types of files (such as images). Pictures should be scanned and triaged using the Picture Finder option.

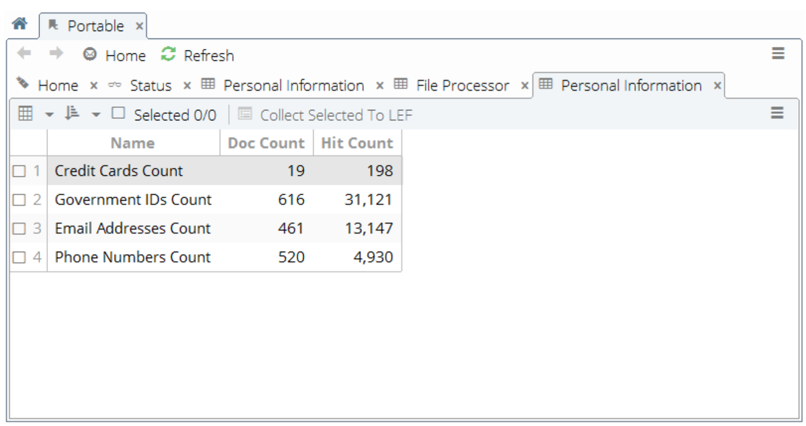
Processing Files Using Keyword Finder

Keyword Finder processing lets you see a list of documents containing keywords, as they are found.

Options for Keyword Finder are configured when the job is created using the File Processor module.

> **Note:** The results returned by the Keyword Finder may appear to be significantly different from the results returned when using the EnCase Evidence Processor. This is because the EnCase Evidence Processor lists all hard link entries for a given file, while the Keyword Finder detects that a given set of entries are all hard links to the same file and lists only one from the set. Also, Keyword Finder searches transcripts when available, whereas EnCase Evidence Processor performs only a raw search on non-transcript files.

While this module is running, if the job has been configured to triage results, the progress screen can be viewed by clicking the link in the status column of the status dialog.



- The keywords listed in the Keyword Name column are the keywords entered when the job was created.
  - The name for the keyword may be different from the keyword expression being used to search. This is useful when the search expression is a GREP expression or in a foreign language.
  - The table is sorted in alphabetical order based on the Keyword Name.

- The number of documents found to contain at least one instance of the keyword is listed in the Document Count column.
- The number of search hits for the keyword is listed in the Keyword Hits column.
- The Keyword Expression is the literal string used in the search.

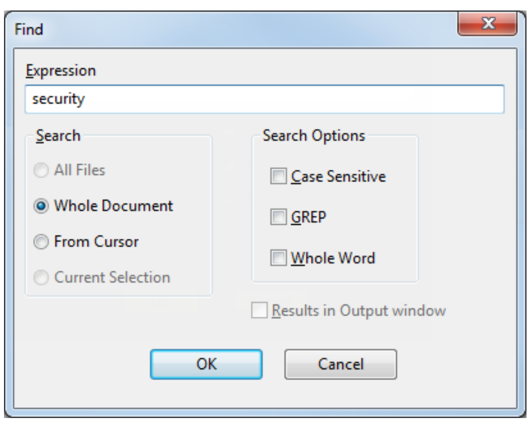
- Columns can be sorted by double clicking the column header. As in EnCase, shift clicking on multiple columns creates multiple layers of sort orders.

Clicking a keyword opens a documents table.

The table shows the document name, the number of times the keyword was found within it, the file size, and its path.

Clicking a link opens a document viewer with keywords highlighted in yellow.

- Click **Next** or **Previous** to open up the next or previous document in the list, using the current viewer.
- Click the checkbox next to **Add to Collection** to add this document to your collection of data. This collection can be turned into a LEF from the status window when your analysis is complete. See Collecting Evidence from Triaged Results on page 364.
- **Fit to Page** adjusts the text to better fit the frame of the dialog.
- You can toggle between either **Full View** mode, with each line numbered, or **Compressed View** with just the lines of the document that contain keywords displayed. When in compressed view, click **Full View** to switch to the full document. When in full view, click **Compressed View** to show only the lines that have keyword hits.
- In Full View, use **Next Hit** and **Previous Hit** to jump to the next highlighted keyword in the document.
- Clicking **Find** opens a dialog that lets you search for additional expressions. From here, you can search for the expression within the current document, within the current document from your current position to the end, or within the currently selected text.



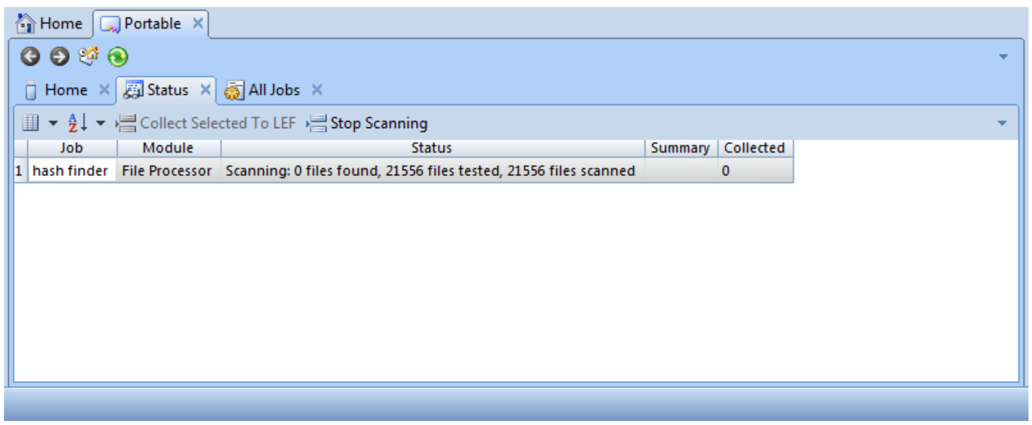
Processing Files Using Hash Finder

The Hash Finder searches for files by comparing their hash values to hash values found in either a new or pre-existing hash set. This option creates a new hash set or uses a pre-existing set.

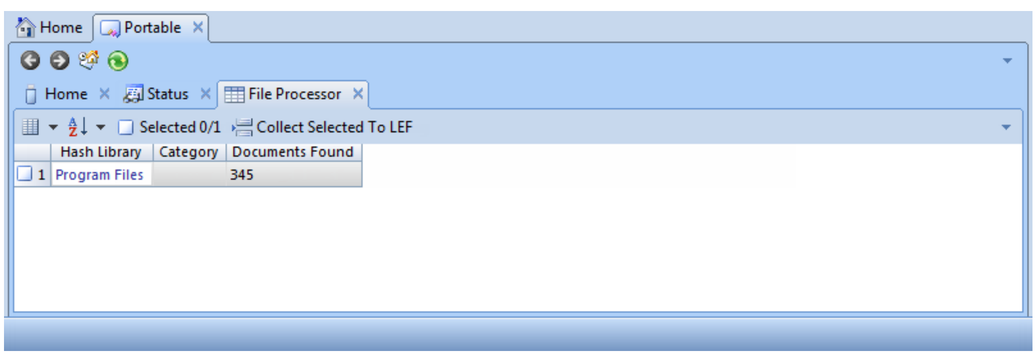
> **Note:** You cannot use the Hash Finder unless your hash libraries are correctly set up.

Options for Hash Finder are configured when the job is created using the File Processor module.

While this module is running, you can view the progress in the **Status** tab.



If the ability to triage results was selected when configuring the job, you can click on the link in the status column to open up a search results tab.



- Hash Library displays the name of the hash set library used in the module.
- Category is the category assigned to that library.
- The Document Found column displays the number of documents found to have hashes that match those in the hash library.

Clicking the hash library link opens up the document table, displaying all documents that match the hash values in that library.

Processing Files Using Picture Finder

Picture Finder processing searches for picture files greater than a designated size. The default Triage Pictures job included with the standalone version of EnCase Portable is set to display pictures greater than 10KB only. You can change this option after the job is created.

Options for Picture Finder are configured when the job is created using the File Processor module.

While this module is running, the progress screen can be viewed by clicking the link in the status column of the status dialog.

VIEWING

You can increase or decrease the size of your images, by changing the number of rows and columns you are viewing.

To see fewer, larger pictures, decrease the number of columns by clicking **Fewer Columns**. To see more, smaller pictures, increase the number of columns by clicking **More Columns**.

You can also increase or decrease the number of rows displayed by right clicking within the gallery and selecting **More Rows** or **Fewer Rows**.

To refresh the screen while a job is running, click **Refresh**.

If an image is corrupt, or if an image type is not supported by EnCase, its thumbnail does not display.

SORTING

Images are initially displayed in the order they are found.

EnCase Portable provides a quick sorting function that brings pictures in popular locations to the top for efficient review. After the search has completed, click **Add Sort** to apply sort priority to pictures located in the User folder(s), then removable media, and then the rest of the drive (s). In addition, multiple images contained in a single folder are sorted by file size, from largest to smallest.

To revert to the found-order sort, click **Remove Sort**.

> **Note:** Images can be added to reports during collection, only. See the Analyzing and Reporting on Data chapter for details.

Triaging Personal Information

The Personal Information module can be configured to see potentially relevant documents prior to them being collected. The module can also be configured to prepare a report of potentially responsive items. These configuration options are selected when the job is created.

When configured for triage, the results screen can be viewed by clicking the link in the status column of the status dialog while a job is running.

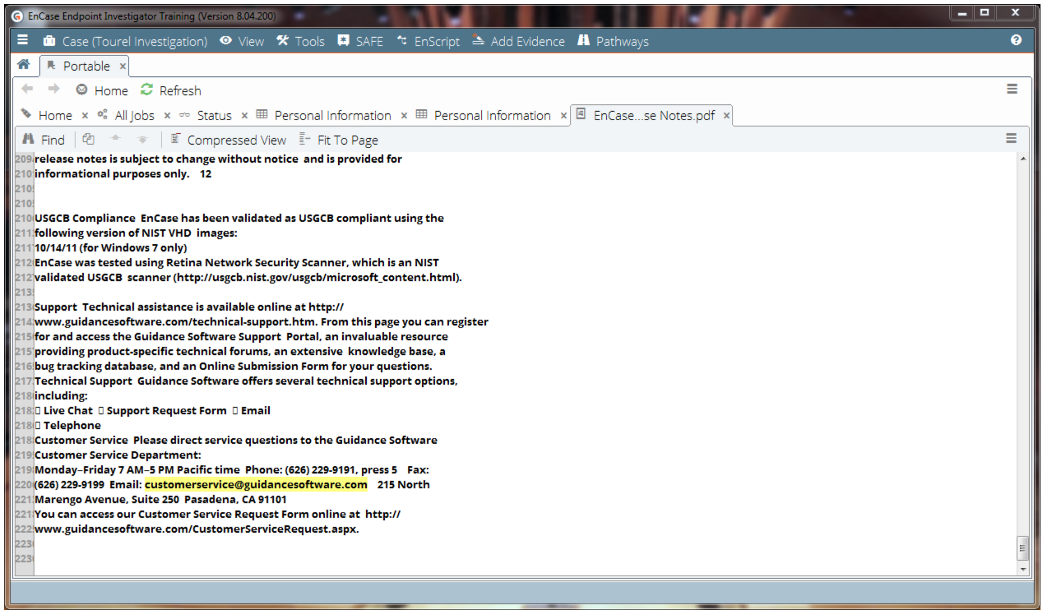
- The personal information types listed in the Keyword Name column are the types of personal information specified by the Personal Information module.
- The number of documents found to contain at least one instance of the personal information type is listed in the Document Count column.
- The number of search hits for the personal information type is listed in the Keyword Hits column.

Clicking a personal information type opens a documents table for that information type.

The table also includes the document name, the number of times the personal information type was found within it, the file size, and its path.

> **Note:** The search hits for credit card numbers are not validated before appearing in this table. Therefore, there may be a discrepancy between the number of hits shown in the document viewer, and the number of actual, verified results.

Clicking the link opens a document viewer with keywords highlighted in yellow.



- Click **Next** or **Previous** to open the next or previous document in the list, using the current viewer.
- Click the checkbox next to **Add to Collection** to add this document to your collection of data. This collection can be turned into a logical evidence file (LEF) from the status window when your analysis is complete. Even if no files are collected, the module can capture and save a complete report of relevant documents for later examination. See Collecting Evidence from Triaged Results below.
- **Fit to Page** adjusts the text to better fit the frame of the dialog.
- You can toggle between either **Full View** mode with each line numbered, or **Compressed View** with just the lines of the document that contain keywords displayed. When in compressed view, click **Full View** to switch to the full document. When in full view, click **Compressed View** to show the lines that have keyword hits only.
- In Full View, use **Next Hit** and **Previous Hit** to jump to the next highlighted keyword in the document.
- Clicking **Find** opens a dialog that creates searches for additional expressions. From here, you can search for the expression within the current document, within the current document from your current position to the end, or within the currently selected text.

Collecting Evidence from Triaged Results

When triaging any job, you can select specific files as they come in and save them to a logical evidence file (LEF).

1. Drill down from the status window into the results for each module and select each file to collect.
2. Return to the main status screen.
3. Click **Collect Selected to LEF**. All checked items are collected into a logical evidence file (LEF) and stored with an .L01 extension in the \EnCase Portable Evidence\<Job Name> folder on the storage device.

Copying Evidence

You can copy evidence easily from one location to another. This may be useful for moving evidence from an older version to a new storage location.

To copy evidence:

1. In EnCase select **EnScript** > **Portable Management**. The Portable Management dialog displays.
2. Click the **Evidence** tab.
3. Select the evidence file(s) to copy.
4. Check **Add evidence to case**.
5. To remove the files from the original location, check **Delete evidence after copy**.
6. To change the destination of the copied evidence, enter or browse to a different folder.
7. Click **Copy**. A status dialog displays the files being copied.
8. When finished copying, click **Finished**.

Analyzing and Reporting on Data

After a job is completed, you have two options for analyzing from within EnCase Portable Management or EnCase Portable. Use the **Analysis** option on the Portable **Home** tab to perform an analysis from within a set of interlinking data browsers that lets you drill down into your collected information. Alternately, use the **Advanced Analysis** option to use the EnCase Analytics functions.

ANALYSIS REPORTS

Instead of showing views of artifacts collected, analysis reports attempt to indicate what happened on the system. These reports interpret artifacts and may join together multiple artifacts in a single report, such as Windows link files and Registry keys to show files accessed on specific USB devices.

The **Analysis** and **Advanced Analysis** options create customized reports that show your data organized in tables. You can create reports from within EnCase Portable or from Portable Management in EnCase.

The reports compiled are available only as long as you have the application open. To preserve your information, you can print or export it.

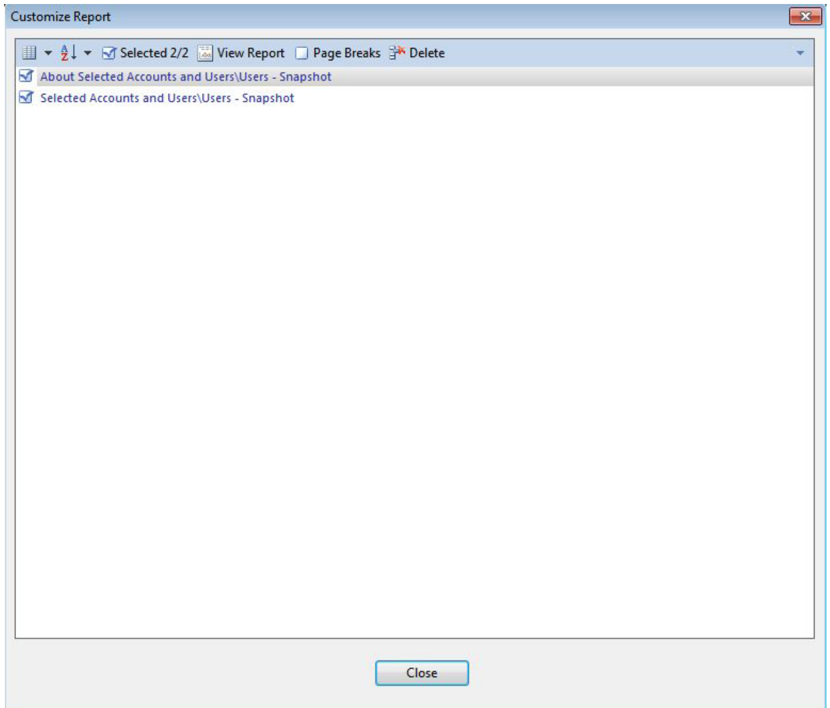
Selecting Target Databases

When more than one target has been collected, multiple databases are created, one for each target. When opening **Advanced Analysis**, the Analysis Target Selector window opens, allowing you to select the target database to analyze.

Creating a Report

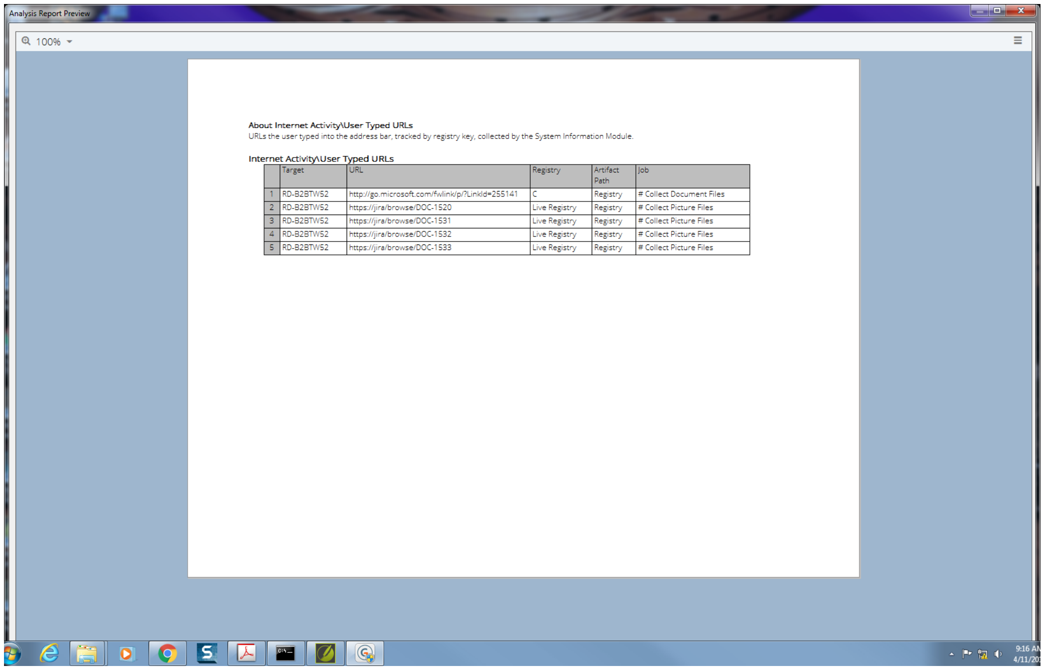
You can create reports from the evidence you have collected.

1. From the EnCase Portable Home screen, select **Analysis** or **Advanced Analysis**. See the discussion in the Overview section of this chapter to determine which is appropriate for your reporting needs. In general, **Advanced Analysis** gives you many more elements to choose from to build your report.
2. The analytics query selector screen displays.
   - Analytics query groups are displayed in the left pane.
   - Select an analytics query group to show results in the right pane.
   - Select results from these queries in the right pane to be added to your report.
3. Double click the analytics query group folder icons to display the analytics queries.
4. Click **Save Selected** in the table toolbar to save the queries. The Set Table Title dialog displays.
5. Enter the title you want for the table in your report and click **OK**.
6. Click **Manage Saved Reports** in the analytics query selector screen to display the tables which have been added to your report. All tables are displayed in the Customize Report dialog.



7. Continue using the analytics query selector screen to add additional query results to your report. You can add as many tables as necessary to your report.
8. Click **Unavailable Views** to display the sets of analysis results that are not yet available, given the collections still under examination. This list can be used as a checklist to assure that the required data is collected.

Click **View Report** to preview your report. From the preview screen, you can also print your report to maintain an artifactof this evidence.

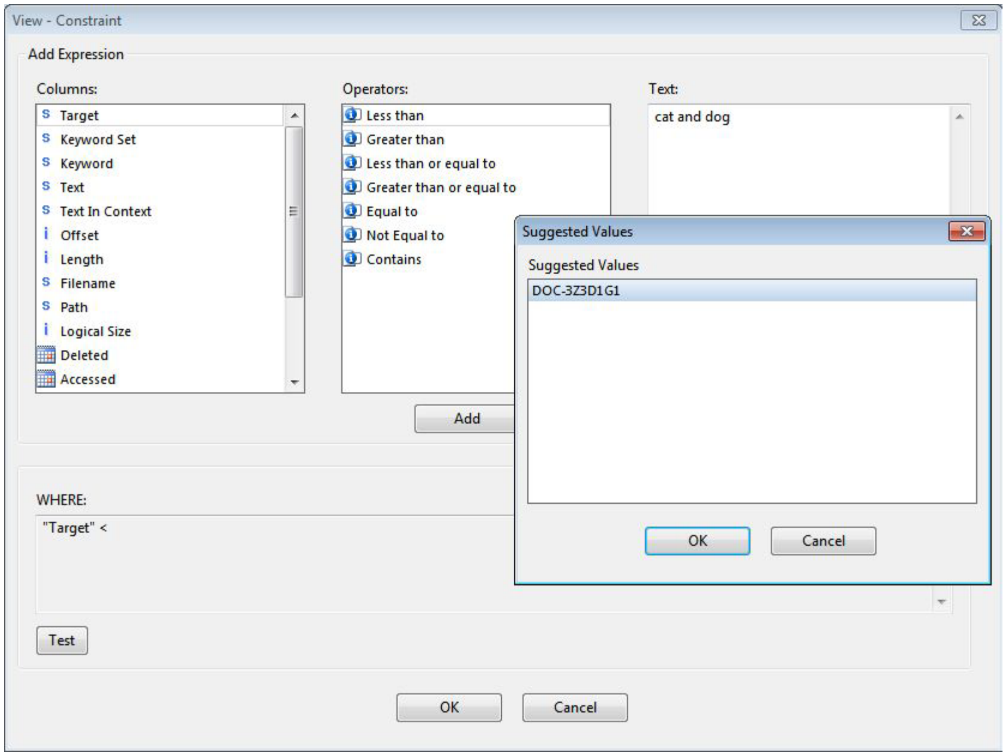


This report structure is discarded after closing.

Adding Constraints to Analysis Data

When analyzing data, you can add constraints to the information that displays in the analytics query selector screen. This option is available only in tables that contain data where a constraint is useful.

1. From an appropriate table in the analytics query selector screen, click **Constraint**.
2. The Constraint dialog displays, showing fields that are relevant to that specific table.



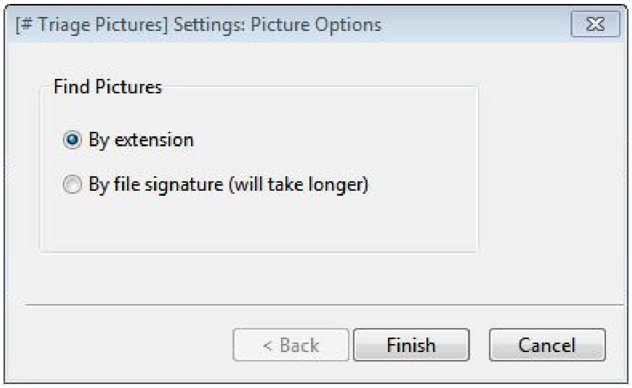
3. Enter the information to include in the table in the appropriate text box. For example, to see filenames that contain the word `Cat` only, enter `Cat` in the Filename text box.
    - Only one value can be entered in each text box. For example, if you enter `Cat and Dog`, to display information that contains both the words `Cat` and `Dog`, EnCase Portable takes the value literally and displays information that contains the entire phrase `Cat and Dog`.
    - If you enter values in multiple text boxes, EnCase Portable displays the information that contains all specified values only.
    - All non-string fields (such as IP addresses, numbers, hashes, or dates) look for exact matches. For example, if you enter 80 for the local port, EnCase Portable looks for port 80 only; port 8080 does not match the filter and will not be displayed.

4. Click **OK**. The table is displayed according to the restrictions entered. The current criteria are shown in the bottom left status area of the Analytics Query Selector.

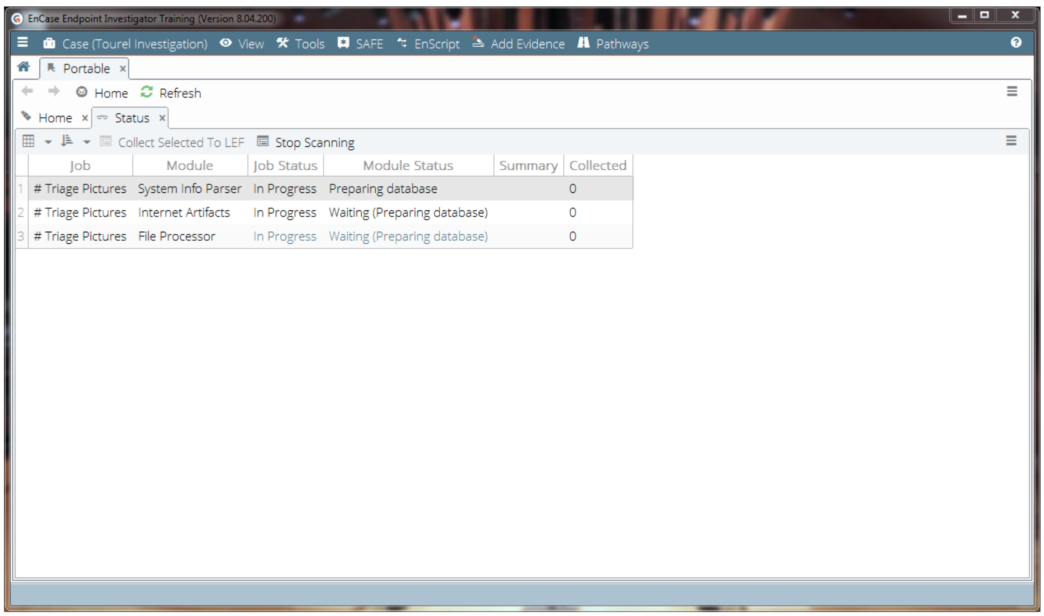
    Note: To remove the restrictions, click **Remove Constraint** in the Analytics Query Selector toolbar.

Adding Images to Reports

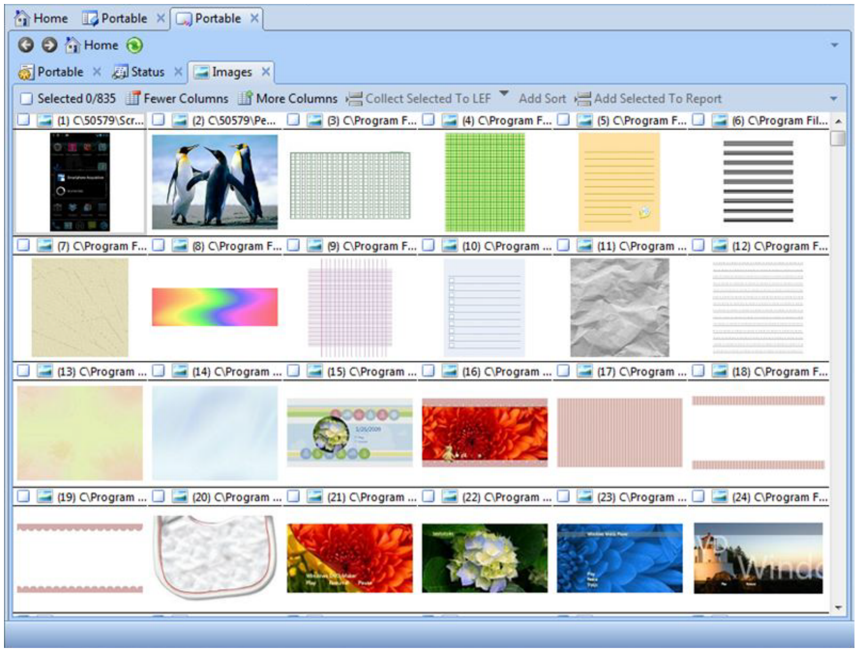
1. From the Portable home screen, run the **# Triage Pictures** job. The Settings: Picture Options dialog displays.



2. Select a Find Pictures option and click **Finish**. Portable displays the **Status** tab.



3. After at least one file is found, click the link in the Status column. This can be done while the job is running. Portable displays the **Images** tab.



4. Select images to add to your report by clicking individual image check boxes.
5. Click **Add Selected To Report**. The Customize Report screen displays, listing the images selected.
6. Select **View Report**. Your report now displays the images.
7. To print a report, select the hamburger menu at the upper right and click **Print**.

Images can be added to a report only while the **# Triage Pictures** job is running. However, if you select **Collect File Contents** in the File Processor wizard, image data in the LEF can be added to reports from EnCase.

Snapshot Reports

Snapshot Reports contain structured information on processes, open files, users, and ports. Snapshot Reports can help you determine precise relationships between parent and children processes, details about processes and their associated DLLs, and open ports and their associated processes and DLLs. Using Snapshot Reports, you can determine which process instance spawned the process you are trying to identify. These reports allow you to see the path, command line parameters, and DLL/EXE file information for specific running processes.

Clicking an entry in the Parent Process ID column, which contains process IDs for each parent process instance, displays all running instances of the process. This filters the report to display matching process IDs, only, which allows you to trace that process to its source. For example, instead of displaying only the type of process, such as explorer.exe, clicking an entry in the

Parent Process ID column displays information on all instances of explorer.exe. Similarly, clicking a number in the Children Processes column displays detailed information for all the children processes associated with the process instance.

Snapshot Reports also display both port information and its relationships to process instances and DLLs, so you can determine which DLLs are active as well as which process instance loaded each DLL.

Some Snapshot Reports combine information from other reports to make the workflow more efficient. Under **Operating System** > **DLLs**, the **DLLs by Process Details** Report combines all the information in the DLLs Report and the Processes Report. Under **Network**, the **Open Ports by DLL** Report combines all the information in the DLLs Report, the Processes Report, and the Open Ports Report. Under **Operating System** > **Processes**, the **Processes** report combines all the information in the DLLs Report and the Open Ports Report.

Each Snapshot Report also has an **About** option which shows details for each report.

To use these features, make selections in columns in the following reports:

DLLs by Process Details: Instance Name, Parent Process ID, Open Ports, and Children Processes.

Open Ports by DLL: Instance Name, Parent Process ID, and Children Processes.

Processes: Instance Name, Parent Process ID, Open Ports, Children Processes, and DLL Count.

These Snapshot Report columns provide the following information:

Instance Name is a descriptor for a specific instance of a process. An instance name is often the same as a process name.

Children Processes are the processes that were spawned by a parent process. For example, some malware spawns many other processes. Viewing a malware parent process shows how many processes it created. This count is displayed as a link to the child processes.

Open Ports are ports that have been opened by a process to communicate over the network. These include both local and remote ports.

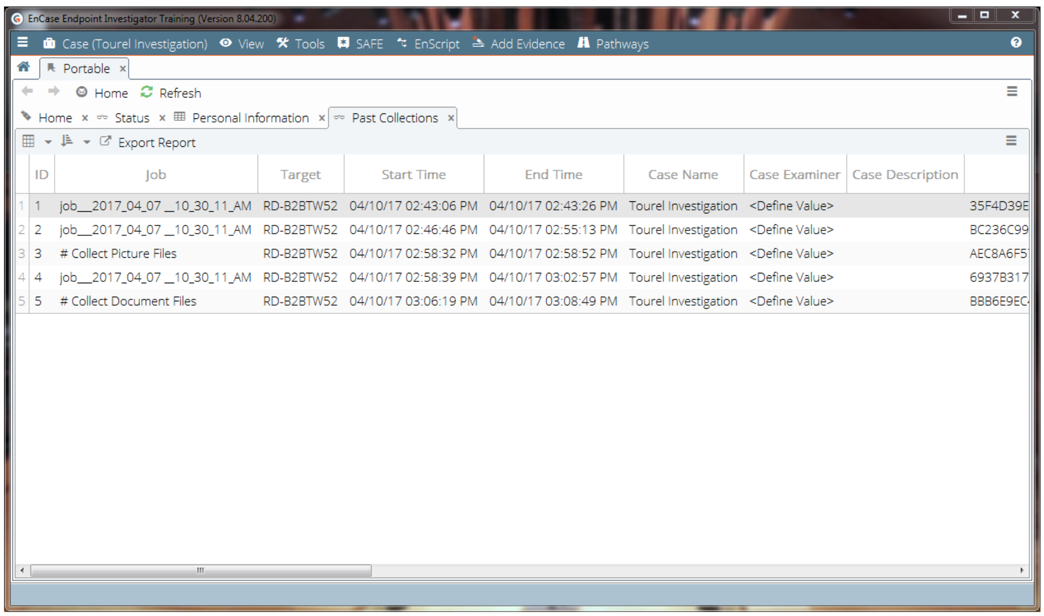
DLL (Dynamic-linked library) Counts are used by many programs to share code. Malware can inject a malicious dll and a program will execute it without realizing it is malicious code. The DLL Count is the number of dlls that a specific program is using.

Exporting a Report

You can run a report that shows comprehensive details of all the jobs and scans previously run on the current Portable device.

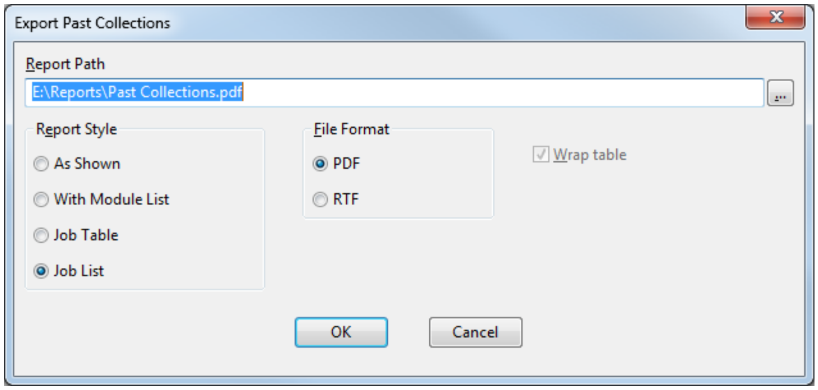
From the Portable home screen:

1. Click **Past Collections**. The **Past Collections** tab displays.



   - Using the Column options on the left, hide or show columns to suit your requirements.

2. Click **Export Report**. The Export Past Collections dialog displays.



3. Select or verify the output path for the report.
4. Select your report style.
    - **As Shown** exports the report as it appears on the screen.
    - **With Module List** exports the report with the modules displayed by name in a single column.
    - **Job Table** (default) exports the report with the rows and columns in the same orientation as displayed in the tab. This results in a wider report.
    - **Job List** exports the report with the rows and columns transposed from the way they are displayed in the tab. This results in a taller report.
5. Select your file format.
6. If enabled, select **Wrap table** to export the columns at full width. If unchecked, the contents within the columns will wrap and the columns will be compressed so the table fits on one page.
7. Click **OK**. The report outputs to the designated report path.

Maintenance

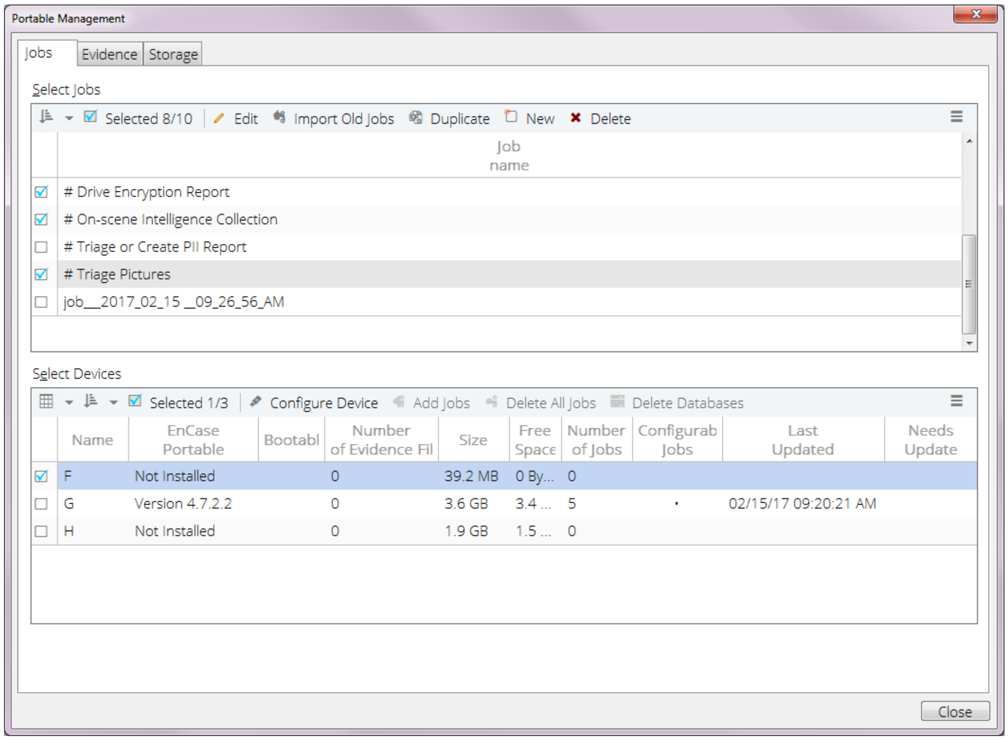
The following section contains topics on portable device maintenance, including preparing portable devices and storage, modifying EnCase portable device configuration, and preparing additional USB storage devices.

Preparing Portable Devices

You can create Portable devices out of any removable storage device. Portable devices can run from any EnCase Forensic or EnCase Portable license.

To prepare a Portable Device:

1. Select **Tools** > **Create Portable Device**. The Portable Management screen displays.

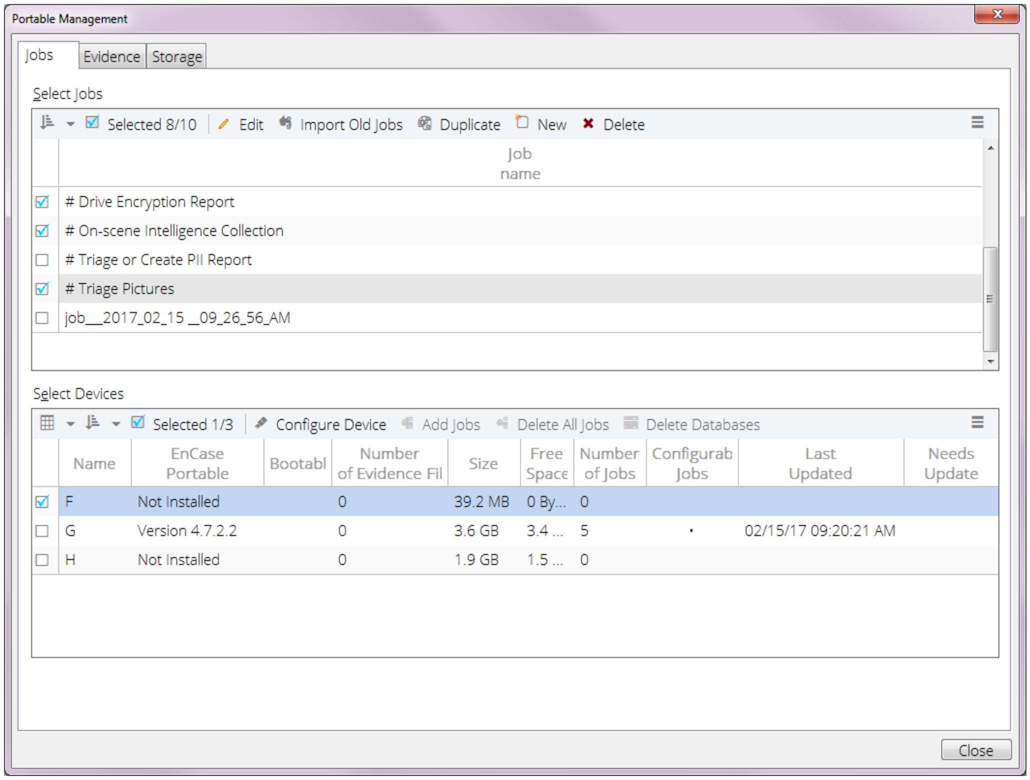


2. Select a device and click **Configure Device**. A status screen displays the updates to the device as they are being executed.
3. When done, click **Finished**. The device is labeled with the currently installed version.

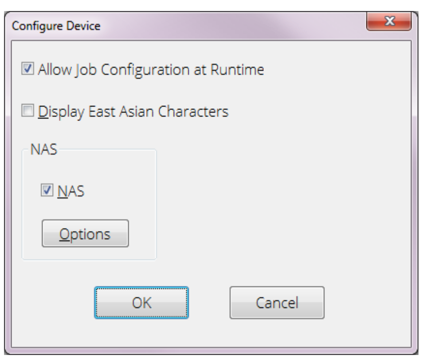
Modifying the EnCase Portable Device Configuration

The Portable device can be configured to determine how jobs are executed.

1. Select **Tools** > **Portable Management**. The Portable Management dialog displays.



2. Select the drive to configure and click **Configure Device**. The Configure Device dialog displays.



- **Allow Job Configuration at Runtime** enables the user to create and edit jobs in the field, using the Portable device. By default, this option is enabled.
- **Display East Asian Characters** enables the display of Unicode character sets, specifically for East Asian language support.
- **NAS** licensing enables the use of EnCase Portable without a separate security key.

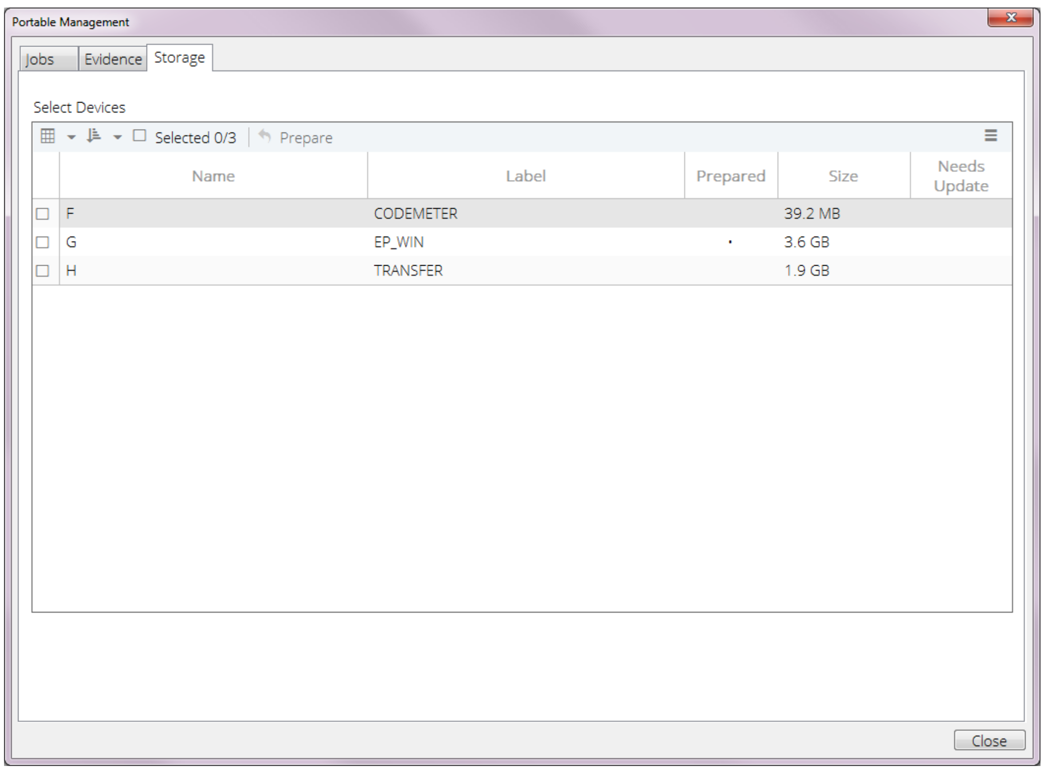
3. When done, click **OK**.

Preparing Additional USB Storage Devices

The storage device that comes with EnCase Portable is ready to use. If you choose, you may use other USB storage devices for use with EnCase Portable by adding a specific folder structure to the device.

To prepare a USB storage device for use with EnCase Portable:

1. Insert the storage device into the computer.
2. Select **Tools** > **Portable Management**.
3. Click the **Storage** tab. All devices that require preparation are indicated.



> **Note:** If there is a bullet in the Needs Upgrade column, the device needs to be restored.

4. Select one or more devices and click **Prepare**. A dialog shows the status of the task. When complete, this dialog confirms the creation of the EnCase Portable Evidence folder on the storage device.
5. The Prepared column displays a dot when the process is complete.

Configuring EnCase Portable for NAS Licensing

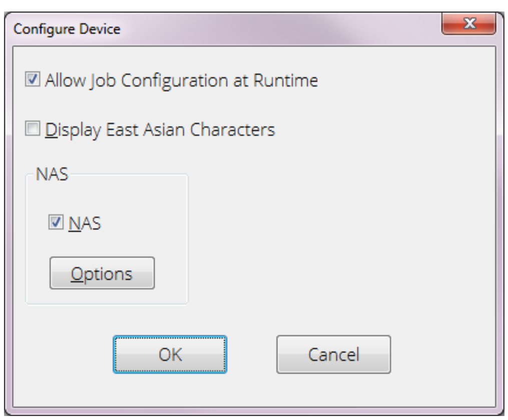
You can run EnCase Portable from any 4 GB (or greater) USB device without a security key by using the Guidance Software License Manager. License Manager is a Network Authentication Server (NAS) and enables the distribution of EnCase Portable licenses across the network. This functionality is available only when you purchase Portable enabled through License Manager. Please contact your sales representative for more information.

To work with the NAS:

- EnCase Portable must be used on a target computer that has routable network access to License Manager.
- The EnCase Portable EnLicense must be stored in at least one of the following places to work with License Manager:
  - In the `\EnCase Portable\License` folder on the examiner machine used to configure the EnCase Portable NAS settings (default location).
  - In the `\SAFE\License` folder on the SAFE (recommended).

Guidance Software recommends storing the EnLicense on the SAFE so multiple machines can be set up without a specific local licensing folder. If an EnLicense cannot be found in either of these locations, Portable must have a physical security key.

1. Select **Tools** > **Portable Management**. The Portable Management dialog displays.
2. Select the drive to configure and click **Configure Device**. The Configure Device dialog displays.



3. Select the **NAS** checkbox, then click **Options**. The NAS Settings dialog displays.
    - **User Key Path** specifies the location of the NAS key file.
    - **Server Key Path** specifies the location of the SAFE public key file.
    - **Server Address** is the name or IP address of the Network Authentication Server. If you are using a port other than 4445, provide the port with the address (for example, 192.168.1.34:5656).
4. Click **OK**. The prepared USB device can now run as a Portable device.

Troubleshooting

MY JOB HANGS.

Some jobs may take long periods of time to execute. If the progress bar is moving occasionally, the job is still running.

ENCASE PORTABLE WILL NOT LOAD OR RUN.

If the license on the Portable device has expired or is damaged, EnCase Portable will not load and run. Instead, EnCase (Acquisition Mode) displays in minimized form in the corner of your desktop.

Maximize EnCase and check the title at the top. If it displays EnCase Acquisition, the dongle and/or license must be extended or replaced.

WHEN TRYING TO RESTORE PORTABLE I GET A MESSAGE THAT THE DEVICE IS IN USE.

If you are sure the Portable device is not in use, but consistently get a message that the device is busy:

1. Stop all Portable Management and Portable processes.
2. Close EnCase.
3. Remove the device from your computer.
4. Reinsert the device into your computer.
5. Retry the restore procedure.

ENCASE REPORTS THAT I RESTORED AN ENCASE PORTABLE IMAGE SUCCESSFULLY, BUT IT DOES NOT SHOW UP ON THE USB DEVICE.

If you have just restored the image to your Portable device, unplug the device from your system and then plug it back in again. If the device still does not appear, the boot image may have been truncated during the restore process.

The sector size of the restore image and the destination drives must match exactly, or the destination drive must be larger. If the destination drive is even a few sectors smaller than the .E01 restore image, a warning dialog is displayed before the restore starts. If you choose to continue, the restore process is shown as successful even though the target drive image is truncated and data is potentially lost. Guidance Software recommends using a destination drive that is at least 4GB in size.

You should go back through the restore process and make sure the EnCase Portable image has been correctly restored to the physical storage device.

MY MCAFEE SAFEBOOT ACQUISITION IS NOT WORKING.

To troubleshoot this issue, first check to make sure your credentials are accurate and that you are not trying to run a 64-bit version of EnCase. SafeBoot only works with 32-bit versions of EnCase.

Next, make sure that you have the correct files in the correct locations.

The following files must be present in the C:\Program Files\EnCase8\Lib\SafeBoot Technology\SafeBoot folder of your EnCase installation directory:

File/Folder Name
sbAlgs folder [blank]
sbTokens folder
SafeBoot Tool folder
SbAdmDll.dll
SbComms.dll
SbDbMgr.dll
SbErrors.xml
SbFileObj.dll
SbGroupObj.dll
SbMachineObj.dll
SbUiLib.dll

File/Folder Name
SbUserObj.dll
SbXferDb.dll
SafeBoot Tool\GetKey Offline.xml
SafeBoot Tool\GetKey.xml
SafeBoot Tool\SafeBootTool V5.exe
sbTokens\SbTokenPwd.dll

Also, the following files must be copied from your company's SafeBoot server and copied to your local folder structure:

Copy from SafeBoot server	Copy to local machine
C:\Program Files\SBAdmin\SDMCFG.INI	C:\Program Files\EnCase8\Lib\SafeBoot Technology\SafeBoot
C:\Program Files\SBAdmin\ALGS\<Algorithm>\SbAlg.dll	C:\Program Files\EnCase8\Lib\SafeBoot Technology\SafeBoot\sbAlgs

FAQs

HOW DO I UPGRADE MY ENCASE PORTABLE DEVICE?

In Portable Management, a bullet in the Needs Upgrade column indicates that the device needs to be restored.

HOW DOES ENCASE PORTABLE DETERMINE WHAT DEVICE TO USE FOR STORAGE?

After a job finishes, files created from that collection are stored in a predefined location on a configured EnCase Portable storage device. During initialization, EnCase Portable determines the storage location by:

1. Compiling a list of all prepared storage devices.
2. Determining which storage devices are also EnCase Portable devices.
3. Using the first detected storage device.

If the only device found is the Portable device, that device is used for storage.

WHAT FILES ARE CREATED WHEN A JOB IS RUN?

Unless you are collecting logical or physical images of an entire device, information is collected into logical evidence files (LEFs). In addition to creating LEFs, a SQLite database is also created.

When a collection job is run using the File Processor module and the metadata processing type, two LEFs are created. One of the LEFs contains the collected files and is designed to be brought into EnCase so that you can process or view the collected files. The second LEF does not contain any file data, but simply contains meta-information and metrics about the data that was processed and collected. This LEF is not designed to be added to a case in EnCase, but is used by EnCase to generate reports.

CAN I CREATE ENCASE EVIDENCE (.EX01/.E01) FILES WITH ENCASE PORTABLE?

Yes. Evidence files are created when you acquire an entire physical or logical device. This can be done by using the default imaging job supplied with EnCase Portable (#Create Copy of Drive or Memory) or by creating your own job and selecting the Collection\Acquisition module.

WHERE ARE FILES STORED ON THE STORAGE DEVICE?

EnCase Portable uses two types of evidence files:

- Files that contain the actual evidence files that have been collected. These files have either an .Lx01/.L01 or .Ex01/.E01 extension and can be mounted and used in EnCase. They are stored during EnCase Portable collection in `..\EnCase Portable Evidence\`.
- Files that contain summary data about collected information and are used for analysis. These files have an .L01 extension and contain metadata about the collected files. They do not contain the actual evidence files themselves. These files are stored during EnCase Portable collection in `..\EnCase Portable Evidence\ModuleEvidence`.

Each specific target has its own logical evidence file (or LEF), with the name of the target reflected in the name of the logical evidence file. If a target's LEF is already in the storage folder when a new collection is started, you have the option to overwrite the previous data.

The Module Evidence and the File Evidence folders contain folders for each collection job that has been run.

WHERE ARE EVIDENCE FILES STORED WHEN I IMPORT THEM INTO ENCASE?

LEF files created by EnCase Portable are imported by opening the **Evidence** tab in **Portable Management** and selecting evidence to be copied to case folders. By default, the LEFs are stored in the `%\portable` evidence path located in case paths for the open case. The LEFs containing file data can be added directly into EnCase by selecting the checkbox option.

If you choose to add LEFs to EnCase directly from the storage folder, please note that when EnCase Portable collects data, it can collect files (such as when the File Collector module is used) or it can collect parsed data (such as when the Internet Artifacts module is used). To make it easier to conduct examinations, files are stored separately from parsed data. LEFs containing file data can be identified by the words "Collected Files" in the name of the LEF. It is only these LEFs that can be added to and examined with EnCase.

LEFs that contain parsed data are designed to be analyzed in Portable Management and do not have Collected Files in the file name. If you attempt to add these files into EnCase, the collected information will not be viewable.

WHAT FILES ARE COPIED TO THE ENCASE PORTABLE DEVICE DURING EXPORTING?

The following items are copied to the Portable device during the export process:

- EnCase.exe

  Note: When a 64-bit version of EnCase is being used, the 32-bit version of EnCase is copied to the EnCase Portable device.

- EnCase Portable config files (to `\EnCase Portable\Storage`)
- EnCase Portable EnScript (to `\EnCase Portable\EnScript`)
- EnCase config files (to `\EnCase Portable\Config` (`FileTypes.ini` and `FileSignatures.ini`))
- All license files to `EnCase Portable\License` folder
- All cert files to `EnCase Portable\Certs` folder

WILL A 64-BIT VERSION OF ENCASE WORK WITH ENCASE PORTABLE?

Yes. The EnCase 64-bit installer installs the 32-bit files necessary to configure a security key. This includes 32-bit decryption DLLs.

DOES ENCASE PORTABLE WORK WITH LINUX?

EnCase Portable supports Linux-based machines, unless they are using logical volume management (LVM). Any machine with an OS that uses LVM should be able to be acquired and analyzed by the full version of EnCase ForensicEnterprise.

WHEN USING THE FILE PROCESSOR MODULE AND THE METADATA PROCESSING TYPE ON A RUNNING MACHINE, DOES ENCASE MOUNT LOGICAL OR PHYSICAL DEVICES FOR ANALYSIS?

EnCase Portable mounts the logical device when used on a running machine.

HOW ARE DOMAIN VISITS COUNTED? BY SUMMING HISTORY ENTRIES, CACHE ENTRIES, BOTH?

Domain visits are computed by summing the history entries only.

HOW ARE DAILY AND WEEKLY RECORDS FOR INTERNET EXPLORER HANDLED?

In the analysis table report, you do not see the history grouped into daily and weekly folders as IE and EnCase. Instead, you start with high level domain visits and drill into the individual entries by navigating from there.

MY NUMBERS SEEM WAY OFF. SHOULDN'T THE COLUMN BE CALLED HITS INSTEAD OF VISITS?

Visits are pulled from the cache file directly, and to prevent confusion, the name is not changed.

WHICH GREP EXPRESSIONS ARE BEING USED TO PERFORM CARD, E-MAIL, AND SSN SEARCHES?

Visa-13	[4][#]{12,12}
Visa-16	[4][#][#][#][^#]?[#]{4,4}[^#]?[#]{4,4}[^#]?[#]{4,4}
MasterCard	[5][1-5][#][#][^#]?[#]{4,4}[^#]?[#]{4,4}[^#]?[#]{4,4}
American Express	[3][47][#][^#]?[#]{7,7}[^#]?[#]{5,5}
Discover	[6](([0][1][1])|([5][#][#]))[^#]?[#]{4,4}[^#]?[#]{4,4}[^#]?[#]{4,4}
Email	[a-z0-9\~_\.\x2D]+@[a-z0-9_\x2D]+\.[a-z0-9_\x2D\.]+
SSN	###[\x2D]?##[\x2D]?####
Phone with Area Code	[(][#]{3,3}[)] ?[#]{3,3}[\x2D][#]{4,4}
Phone without Area Code	###[\.\x2D]####

ARE THESE GREP EXPRESSIONS HARDCODED IN THE PERSONAL INFORMATION MODULE OR CAN WE MODIFY THEM IN CASE WE HAVE TO ADAPT THE SSN FORMAT FOR GOVERNMENT IDENTIFICATION NUMBERS FROM OTHER COUNTRIES?

You can customize GREP expressions for credit card searches. Further customization options will be forthcoming in a future release.

CONSIDERING THAT ON LIVE CAPTURE SCENARIOS WE ARE USUALLY DEALING WITH COMPUTERS THAT ARE ASSUMED TO BE COMPROMISED, WHY IS THE ENCASE

PORTABLE STICK MEMORY WRITABLE BY DEFAULT?

Since you can run EnCase Portable without an external storage drive, the only place to store this data without compromising the system being investigated is on the EnCase Portable drive itself. Thus the EnCase Portable drive is always write enabled.

Also note that the operating system runs entirely in memory (in a RAM drive); therefore, changes made to the running environment do not affect the environment on disk.

CHAPTER 13

GENERATING REPORTS

Overview	389
Bookmarking Data for Reports	389
Triage Report	390
Using Report Templates	397
Report Object Code (ROC)	413
Report Template Wizard	420
Creating Hyperlinks to an Exported Item from Report Templates	424
File Report EnScript	427
Viewing a Report	429

Overview

The final phase of a forensic examination is reporting the findings, which should be well organized and presented in a format that the target audience understands. EnCase adds several enhancements to its reporting capabilities, including:

- Reporting templates you can use as is or modify to suit your needs.
- Capability to control a report's format, layout, and style.
- Ability to add notes and tags to a report.

Case templates in EnCase consist of three parts:

- Bookmark folders where references to specific items and notes are stored.
- Report templates that hold formatting, layout, and style information. A report template links to bookmark folders to populate content into a report.
- Case information items, where you can define case-specific variables to be used throughout the report.

Bookmarking Data for Reports

In EnCase, as you work on a case, you typically discover files, portions of files, and other items of interest and save them as bookmarks. Bookmarks are saved in folders in the case file. The report template links to bookmark folders to populate content into the report. Bookmarks are saved in folders in the case file. When you create a new case and apply one of the supplied case templates, EnCase provides bookmark folders by default. As an example, the basic template provides these folders:

- Documents
- Pictures
- Email
- Internet Artifacts

You can also create your own folders.

To bookmark data into a folder:

1. Select the content you want from any tab (for example, **Entries**, **Artifacts**, or **Search Results**) and click **Bookmark** on the tab toolbar.
2. From the dropdown menu, select the type of bookmark you want to create, enter a name and optional comment, and click **OK**.
3. View your bookmarks in the **Bookmarks** tab.

See Bookmarking Items on page 295 for more information.

Triage Report

The Triage report enables you to customize and quickly generate an investigation report.

This report creates a fully linked HTML report from bookmark folders you create. Each bookmark folder is a separate report section linked together by a table of contents. Each report section can have an associated custom format or be formatted automatically. Each bookmarked item by default includes a separate item report including comprehensive data for that item.

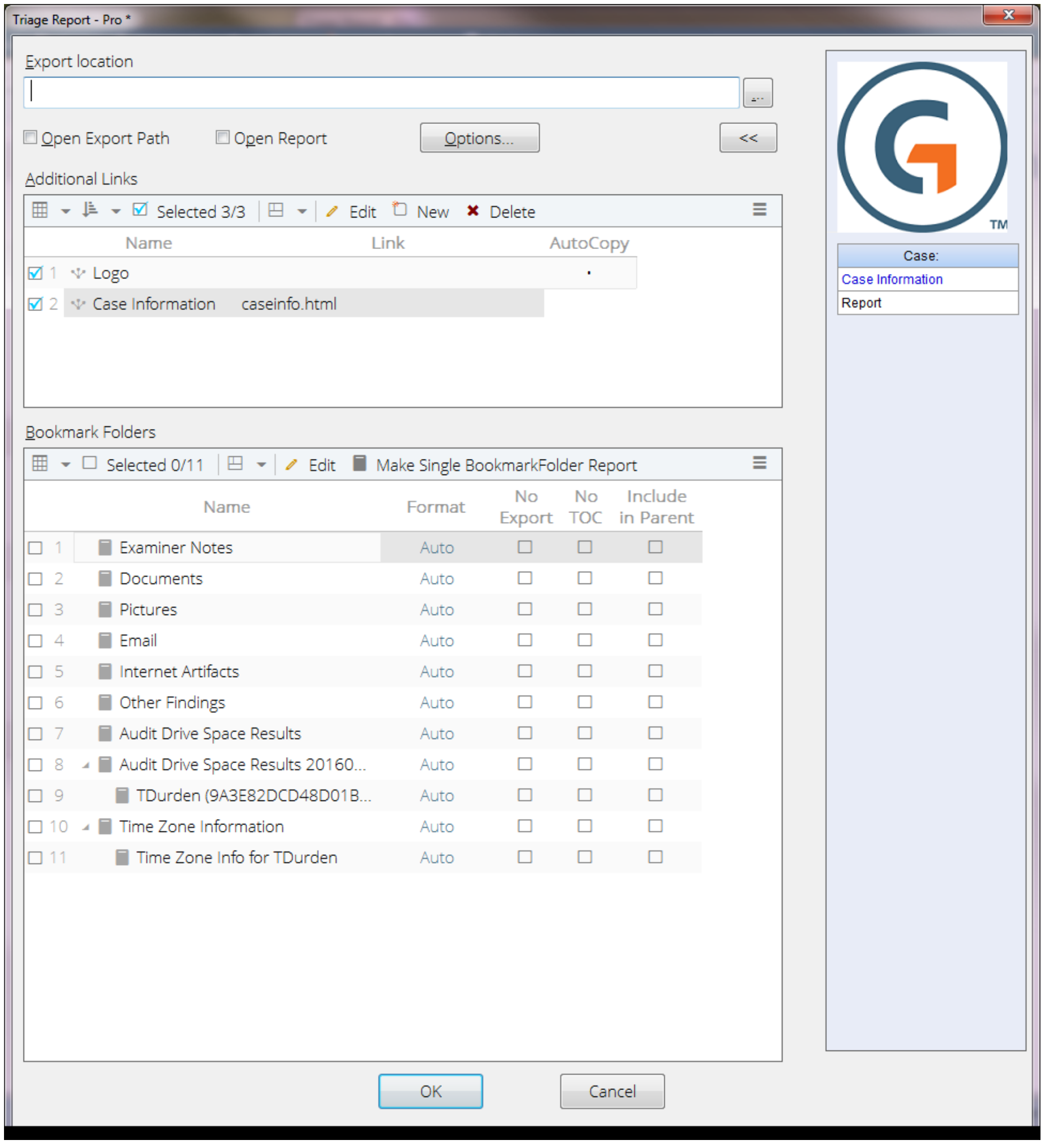
You can customize this report with your own logo, and add external links within the report. All customization can be done using an HTML editor.

When done, this report can easily be distributed on a CD or USB drive and is compatible with most browsers. This enables evidence to be easily shared across teams so that the most relevant information can be discovered and acted upon quickly.

To share your report, navigate to its export location and copy the **Triage Report** folder, `index.html`, and `Triage.Report.html` files to a USB drive or CD.

This reporting option can be accessed on the case home page under the Report header. It is also available in both the Full Investigation and Preview/Triage Pathways.

Main screen



EXPORT LOCATION

Using the browse button, select the folder that the completed HTML report will be placed into. This folder must exist on the system.

OPEN EXPORT PATH

When selected, automatically opens Windows Explorer to the export location when the report is written.

OPEN REPORT

When selected, automatically loads the report in the default browser.

ADDITIONAL LINKS

This section enables the examiner to include additional links in the left pane of the completed report. By default, it includes:

- The Case Information link which draws the data from case information items tab in EnCase.
- The logo item which is used to hold the location for a custom logo.

Unselected items will not show up in the report.

The Name column shows the text that will be placed on the left pane for the link.

The Link column is used to designate the file path of the file to be linked.

If AutoCopy is selected, the linked file will be copied automatically into the export path for the Triage report. This can only be used if the linked file is a single file (i.e. PDF or Word doc, Excel spreadsheet). If the AutoCopy is not selected, you must copy the file or files into the export location before setting the Link field. For example, if you are trying to link in a HTML report which consists of multiple files, the files will have to be manually copied into the export location.

BOOKMARK FOLDERS

The Bookmark Folders table shows all bookmark folders contained in the current case. Selected folders are included in the Triage report when the report is created.

The **Name** field shows the bookmark folder.

The **Format** field designates what information is included in that section of the report. The format can be changed by clicking **Auto** and selecting a different format form the popup box. In the popup:

- The Auto format selection attempts to use the most appropriate data for each of the bookmarked items.
- Selecting **External Link** allows you to set the link on the left side of the screen to an alternate file. If External Link is selected, that report section will not be created. You must manually copy the linked file(s) to the export location before the link is created.

The **NoExport** checkbox stops the exporting of the bookmarked files for that section of the report. Individual files and bookmarks can also be prevented from being exported or included in the report by using the **No Export** and **No Report** options from the Bookmarks tab.

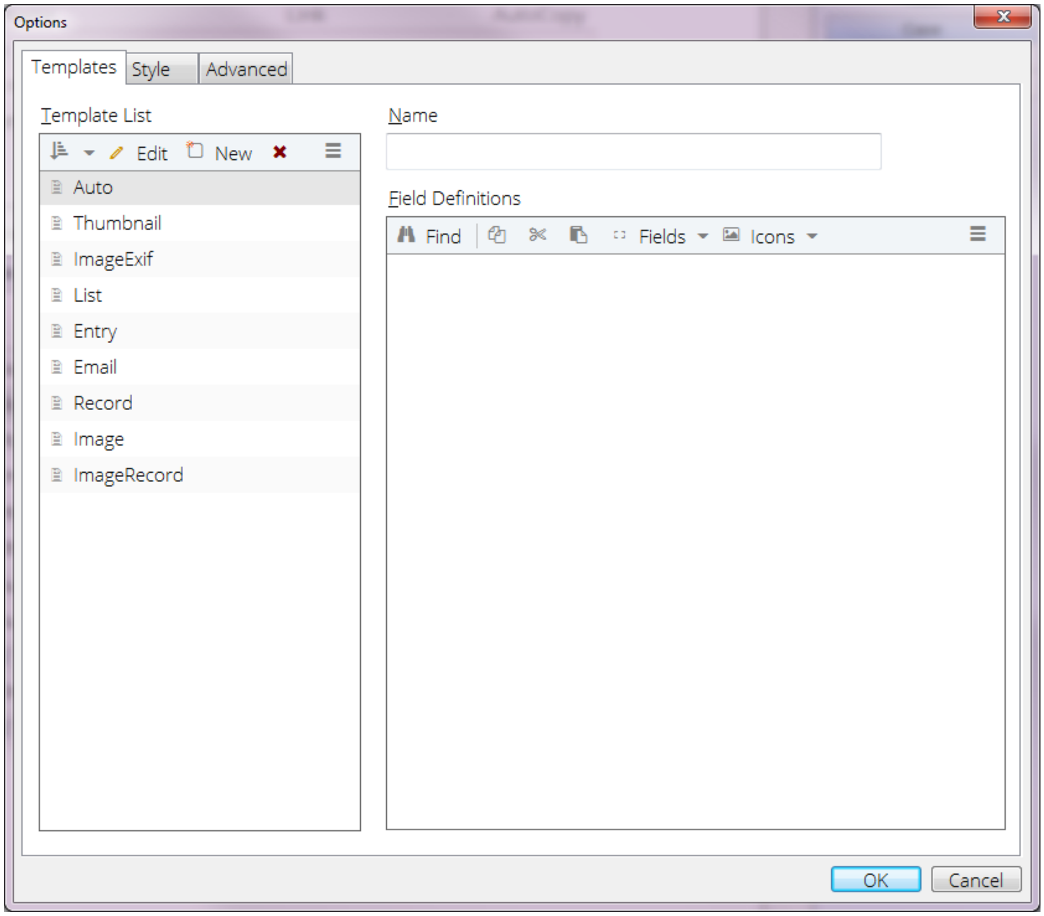
The **No TOC** (No table of contents) checkbox removes that section of the report from the table of contents, but the section is still created and a link is created in the parent report section.

The **Include in Parent** checkbox includes the selected report section within the parent report section. This can be used to create a single report section based on different formats. If you select **Include in Parent** on all bookmark folders, the report will be displayed in a flat form. The HTML links on the left side of the final report will jump the viewer to the respective sections.

Click **Make Single Bookmark Report** on the menu bar to recreate only the current report section. This was designed so you would not have to recreate the entire report when only one section has been changed. This will not recreate the table of contents.

Options

The options button provides you with ways to change the behavior of the Triage report.

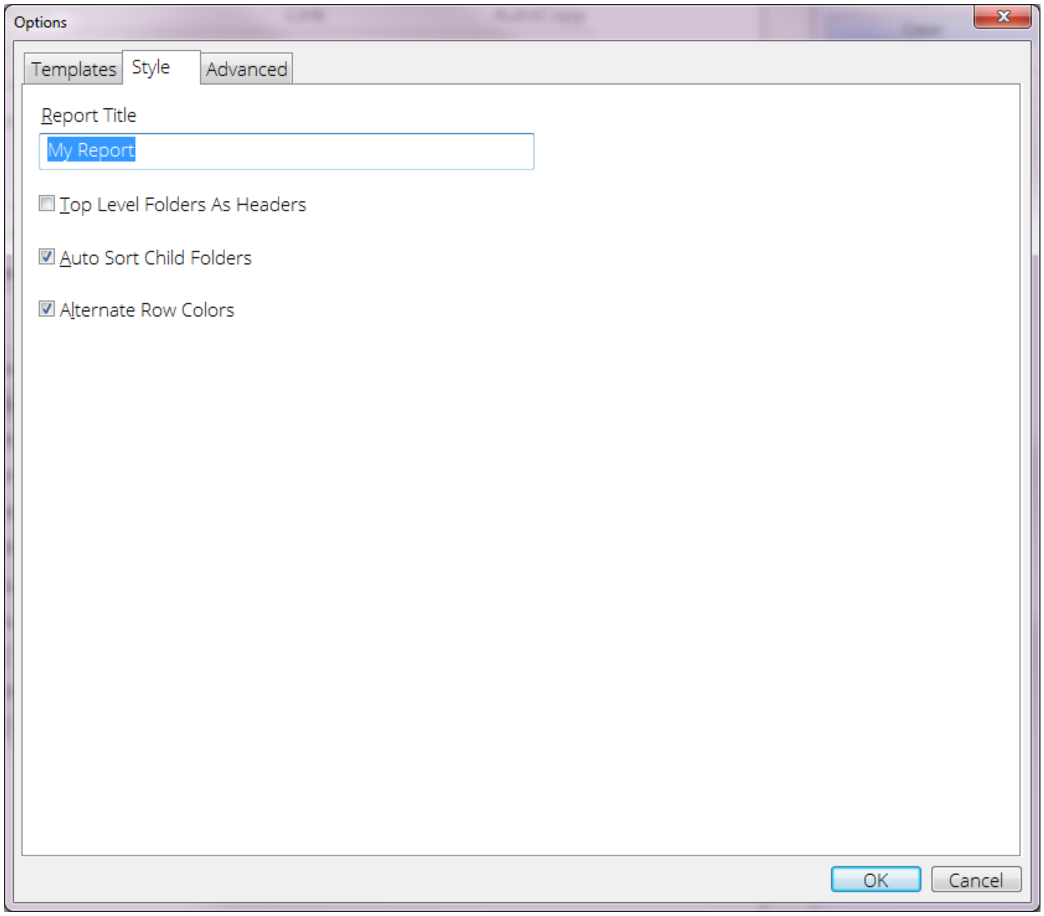


TEMPLATE LIST

The Template List displays the list of default formats and custom formats available. The Auto format automatically selects the default format depending on the bookmarked item type. Default formats can be changed but if they are deleted they will be recreated the next time the Triage report is run.

FIELD DEFINITIONS

Field definitions designate what information is included in the report section for each item.



REPORT TITLE

Enables you to modify the report title shown in the browser when the report is displayed.

TOP LEVEL AS HEADERS

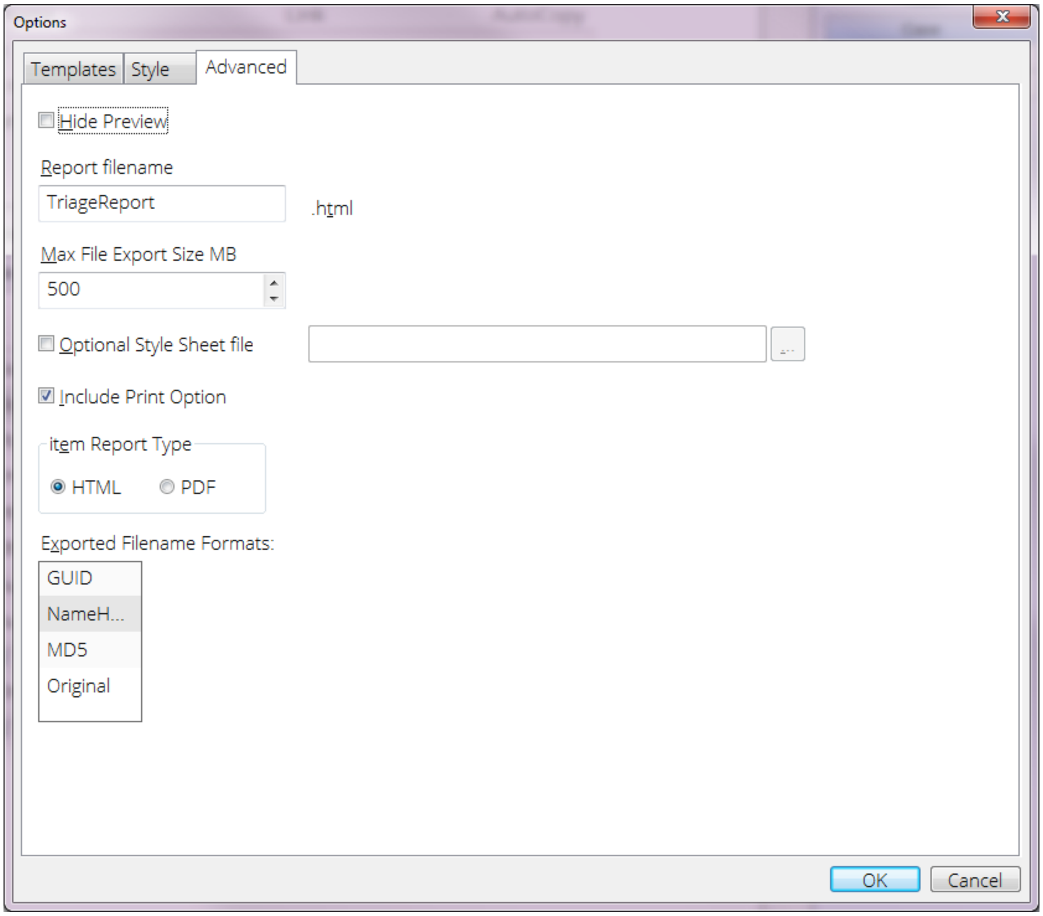
When selected, includes the top level sections in the table of contents even if not selected.

AUTO SORT CHILD FOLDERS

When selected, places the child report sections at the top of the report instead of in the bookmarked order.

ALTERNATE ROW COLORS

When selected, alternates the colors of the rows within the report for better clarity.



HIDE PREVIEW

When selected, hide the preview pane in the main window.

REPORT FILENAME

Enter the filename for the main HTML page. An identical INDEX.HTML is also created.

MAX FILE EXPORT SIZE

Specify the maximum file size that can be exported by the triage report. This feature prevents the unintended export of extremely large files (i.e. pagefile.sys, hiberfil.sys, Unallocated Space).

OPTIONAL STYLE SHEET

Enables you to substitute an alternate style sheet instead of the default.

INCLUDE PRINT OPTION

When selected, includes a print icon at the top of each report section. This option is on, by default.

ITEM REPORT TYPE

Designates if the individual report for each bookmark item (not section) is in HTML format or PDF.

EXPORTED FILENAME FORMATS

Select which type of filename is used for each export file.

Note: The Original setting can cause filename conflicts.

Report Formatting

CUSTOM REPORT FORMATS

- Each line represents a cell of data for the field.
- Separate tags below with a "," comma.
- Use a single dash "-" to make a new line in the table.
- * = default

TAGS

- FIELD= property name. (the word FIELD is not needed) Multiple fields can be place in a single cell, separate with a "|"
- LINK= Defines a hyperlink for the cell. *Auto is a hyperlink to the exported file for the Name property.
- LINK=*AUTO, NONE, FILE,PDF,REPORT,REPORT_HTML,REPORT_PDF, FOLDER
- ALIGN= *1 = left, 0 = center, -1 = right
- HEADER= Alternate cell title, replaces field name.
- ICON= Draws an EnScript icon in the cell
- REPORT,PRINT, etc...
- COLOR= color value in hex or enscript color const - #000066, BLUE
- SIZE= [THUMBNAIL pixels =], [PREVIEW length=100] (not complete)!
- SHOW= BOTH, REPORTONLY (not complete)!

Using Report Templates

A report template is one component of a case template. Each default case template includes a customizable report template. Different case templates can contain different report templates, and each of these templates is completely customizable. In addition to the report template, each case template also includes bookmark folders that are referenced in the report.

Besides the default templates, you can define your own custom reports and save them as part of a case template. For more information, see Using a Case Template to Create a Case on page 79.

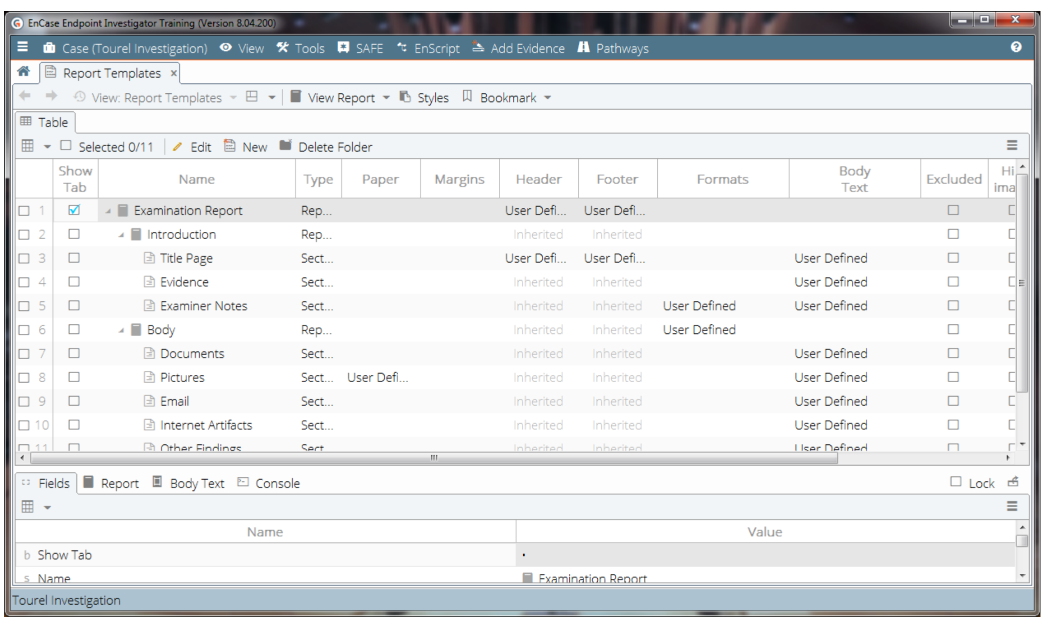
Report Template Structure

Before viewing a report, you need a report template, or outline of what the report will look like. This structure consists of:

- Report sections: groups of similar information and formatting that provide the ability to organize your report.
- Report formatting: page layout, section design, and text styles.
- Report elements: collections of bookmarks. Bookmarks are a key element of the report structure. You do not embed bookmarks into a report template, but embed a reference to the contents of a bookmark folder.

To display the template, click **Report Templates** on the case Home page.

A report component is designated as either a Report or a Section, as shown in the Type column. Typically, Report components contain only formatting information for components beneath them, whereas Section components contain formatting information and Report elements for an individual section. The columns to the right of Type indicate whether a formatting option is user defined or inherited from the component above it in the template hierarchy.



To add new Reports or Sections to the template:

1. Highlight the row above the new element you want to add. Right click and select **New** from the dropdown menu.
2. The New Report Template dialog opens.
3. Enter a Name.
4. Select a Type (Section or Report).
5. If you want to customize Format styles, check the appropriate boxes, or leave the boxes clear to use the default styles.
6. Click **OK**. The new template component displays below the row you highlighted.

Formatting Report Templates

A wide range of formatting options is available for customizing EnCase reports. Guidance Software recommends using the default case templates to start, customizing them as needed, and saving them in a new case template for future use.

Report templates follow a hierarchical tree to simplify formatting. Report sections inherit formatting options from above so that changes to formatting only need to be made in one place.

You can customize these elements:

- Section Name: Used for organizational reference in the template only and does not populate the report.
- Paper: Includes orientation and size.
- Margins: Set values for top, bottom, left, and right margins.
- Header/Footer: Specifies a header and/or footer.
- Data Formats: Specifies how a bookmark displays, including style and content.
- Section Body Text: Specifies the layout and content of each section in the Body Text.
- Show Tab: Determines if this report or section displays in the View Report dropdown menu.
- Excluded: Provides the ability to exclude part of a report.

Configuring Paper Layout

PAPER SIZE AND ORIENTATION

1. Right click the Paper column, then click **Edit** in the dropdown menu. The Paper layout dialog opens.
2. Click a paper size option. This includes options for millimeters or inches.
3. The default orientation is Portrait. Click the **Landscape** checkbox to change the orientation.

4. Click **User defined** to enable the **Page Width** and **Page Height** boxes, where you can specify dimensions manually.

MARGINS

1. Right click the **Margins** column, then click **Edit** in the dropdown menu. The Margins dialog opens.
2. Enter the margins you want in inches. By default, the top margin is 1 inch, the left margin is 0.75 inches, and the right and bottom margins are 0.5 inches.

Localization of Report Layout

Reports in EnCase are designed to work seamlessly in various regions regardless of local preferences such as paper size. If created properly, report templates print correctly on 8 ½" x 11" paper or A4 paper without requiring any changes to the templates.

All reports in EnCase obtain their paper settings from the Windows operating system. Windows stores paper size in the Default Printer settings, so unless a specific paper size is defined in a report template (**Paper** option), EnCase uses the paper size indicated there.

When reports are generated, margins are set for the indicated paper size and the report is rendered in that composition. Users should utilize the ability to set tab stops relative to a specific margin (described above) to ensure that tab stops also scale properly with the different paper variations. Report templates supplied with EnCase are configured in this manner.

Customizing Headers and Footers

You can customize the formatting of headers and footers and what information they contain.

1. Right click the **Header** or **Footer** column, then click **Edit** in the dropdown menu. The appropriate dialog opens.
2. Formatting options (Document, Styles, Case Info Items, etc.) display at the top of the dialog.

Report Styles

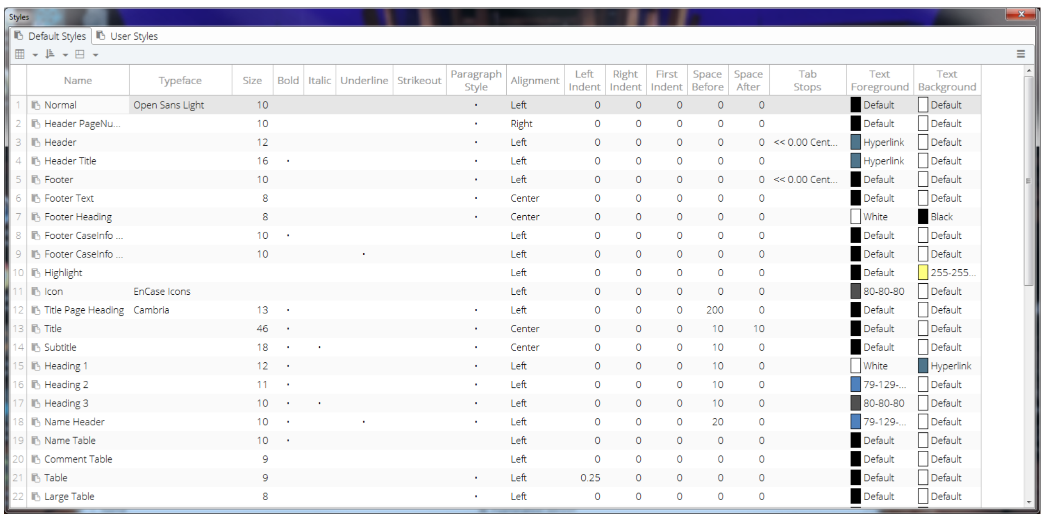
As in Microsoft Word, you use styles to set text formatting options. EnCase comes with many default styles to use in report templates, and you can also create your own styles. To override a default style, create a user style with the same name.

Style options include:

- Font type and size
- Alignment (centered, left and right justified)
- Indentation (left, right, first line)
- Space before/after
- Borders
- Tabs
- Text color
- Background color

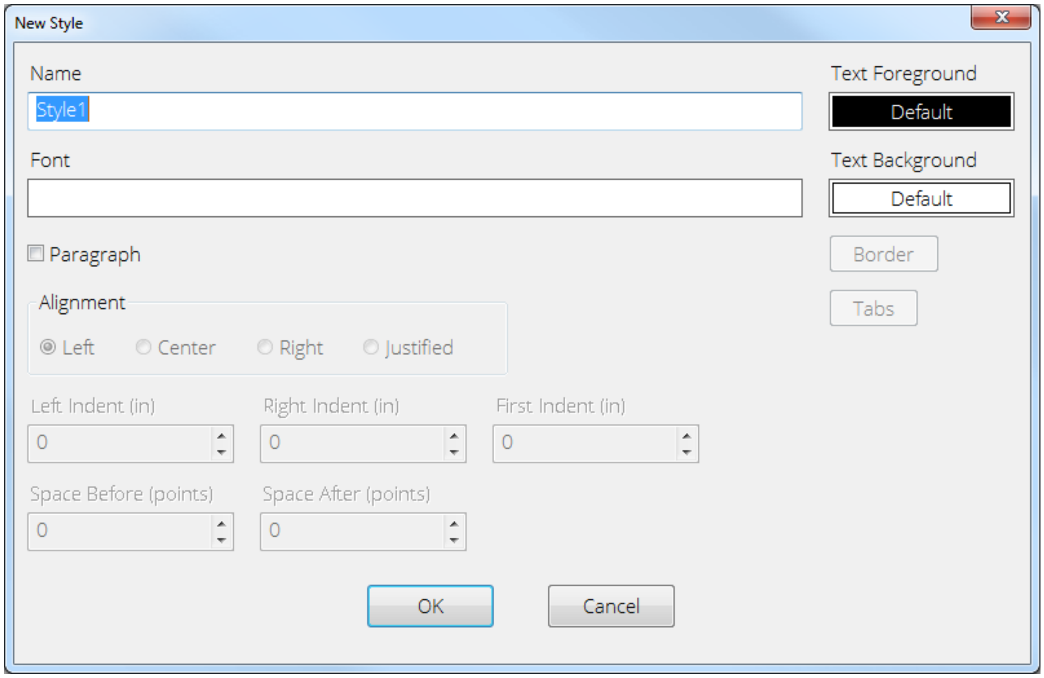
To create a user defined style:

1. In the **Report Templates** tab, click **Styles** in the tab toolbar.
2. The Styles dialog opens, with tabs for **Default Styles** and **User Styles**.



	Name	Typeface	Size	Bold	Italic	Underline	Strikeout	Paragraph Style	Alignment	Left Indent	Right Indent	First Indent	Space Before	Space After	Tab Stops	Text Foreground	Text Background
1	Normal	Open Sans Light	10					·	Left	0	0	0	0	0		Default	Default
2	Header PageNu...		10					·	Right	0	0	0	0	0		Default	Default
3	Header		12					·	Left	0	0	0	0	0	<< 0.00 Cent...	Hyperlink	Default
4	Header Title		16	·				·	Left	0	0	0	0	0		Hyperlink	Default
5	Footer		10					·	Left	0	0	0	0	0	<< 0.00 Cent...	Default	Default
6	Footer Text		8					·	Center	0	0	0	0	0		Default	Default
7	Footer Heading		8					·	Center	0	0	0	0	0		White	Black
8	Footer CaseInfo ...		10	·					Left	0	0	0	0	0		Default	Default
9	Footer CaseInfo ...		10			·			Left	0	0	0	0	0		Default	Default
10	Highlight								Left	0	0	0	0	0		Default	255-255...
11	Icon	EnCase Icons							Left	0	0	0	0	0		80-80-80	Default
12	Title Page Heading	Cambria	13	·				·	Left	0	0	0	200	0		Default	Default
13	Title		46	·				·	Center	0	0	0	10	10		Default	Default
14	Subtitle		18	·	·			·	Center	0	0	0	10	0		Default	Default
15	Heading 1		12	·				·	Left	0	0	0	10	0		White	Hyperlink
16	Heading 2		11	·				·	Left	0	0	0	10	0		79-129-...	Default
17	Heading 3		10	·	·			·	Left	0	0	0	10	0		80-80-80	Default
18	Name Header		10	·		·		·	Left	0	0	0	20	0		79-129-...	Default
19	Name Table		10	·					Left	0	0	0	0	0		Default	Default
20	Comment Table		9						Left	0	0	0	0	0		Default	Default
21	Table		9					·	Left	0.25	0	0	0	0		Default	Default
22	Large Table		8					·	Left	0	0	0	0	0		Default	Default

3. Select the **User Styles** tab.
4. Click **New** in the toolbar.
5. Enter a name for the style and your desired configuration options. Double click **Font**, **Text Foreground**, or **Text Background** to open dialogs for specifying those options.



- Double click **Font** to open the Font dialog, where you can specify:
  - Font face
  - Font style (Regular, Italic, Bold, Bold Italic)
  - Size
  - Effects (Strikeout, Underline)
  - Color
- Double click **Text Foreground** or **Text Background** to open the Color dialog, where you can select a default color or specify a custom color.
- Click the **Paragraph** checkbox to enable other options:
  - Alignment (Centered, Left and Right Justified)
  - Left Indent (in inches)
  - Right Indent (in inches)
  - First indent (in inches)
  - Space Before (in points)
  - Space After (in points)

6. To set a border, click the **Border** button. Set the position, size and color of the border lines you wish to incorporate.

7. To set tab stops within the style, click the **Tabs** button. Right click in the **Tabs** dialog and select **New** to create a new tab.
   - In the **Alignment** box, choose how you want the text to align relative to the tab. Choices are **Left** (left side of the text block is aligned with the tab stop), **Center** (text is centered in relation to the tab) or **Right** (right side of the text block is aligned with the tab stop).
   - Set the **Position** for the tab stop in Inches.
   - In the **Relative** box, set the margin that the tab stop should be relative to. Choose **Left** to position the tab stop a set distance to the right of the left margin, choose **Center** to position it a distance from the center point between the margins, or choose **Right** to position it a set distance to the left of the right margin.

   Note: The ability to set the relative position of the tab enables users to create a report template that you can use with various paper sizes (that is, letter, landscape, A4, etc.) and various orientations (portrait or landscape) without having to reset the margins for the various page widths. Default templates supplied with EnCase are configured in this manner so they can be used in different locales without requiring significant modifications.

8. When you finish, click **OK**. The new style and its attributes display in the User Styles list.

You can also edit or delete an existing User Style.

Modifying Report Template Formats

EnCase now includes the ability to add additional metadata fields for entries and artifacts to report templates. The report template builder makes all entry and artifact fields available and, if selected, the field values display in the report.

You can customize reports by specifying which fields to add to the report template. You can choose to include the value in the field as well as the name of the field. Then, when you generate a report, EnCase includes both specified fields and the content with which they are populated, in the specified area of the report.

All entry, artifact and item (bookmark) fields can be added to report templates. Multi-value fields, such as file extents and permissions, have two options for inclusion: cell and table. Adding the cell data displays the value of the field as displayed within the Entry table view. Adding the table data displays the value of the field as displayed in the **Details** tab.

Inserting a Picture

1. Right click an item in the tree where you want to insert a picture, then click **Edit** in the dropdown menu.
2. The Edit dialog displays. Select the **Body Text** tab, then place your cursor where you want to insert the picture in the Report Object Code.

3. Click **Picture**.
4. The Picture dialog displays. In the Picture dialog, browse to the file you want to insert, specify a size (width and height in inches), then click **OK**.

Inserting a Table

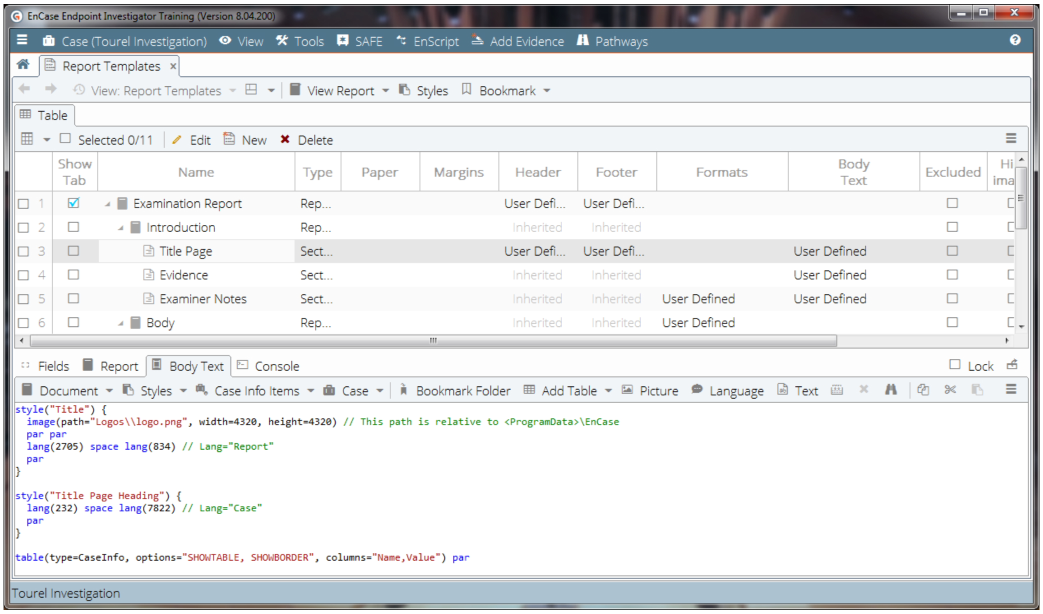
1. Right click an item in the tree where you want to insert a table, then click **Edit** in the drop-down menu.
2. The Edit dialog displays. Select the **Body Text** tab, then place your cursor where you want to insert the table into the Report Object Code.
3. Click **Add Table**.
4. Make a selection from the dropdown list. The dialog for the item you selected opens. The example below shows the Evidence dialog.
    - On the **Columns** tab, click the checkboxes for the columns you want to display.
    - On the **View Options** tab, select the checkboxes for the visual elements you want to display. The tabs and options vary depending on the selection you make from the **Add Table** dropdown menu in step 3.
5. When you finish, click **OK**.

Excluded Checkbox

Depending on your target audience, you may want to exclude parts of a report. For example, an investigator may need to see actual pictures in a report, while another reader does not. You can customize content by clicking the checkboxes in the Excluded column for elements you want to exclude.

Body Text Tab

The **Body Text** tab in the lower pane displays the Report Object Code for a selected object. For example, if you select **Title Page** in the **Report Templates** tab, this code displays:



To add code, use the selectors in the Body Text toolbar:

- Document
- Styles
- Case Info Items
- Case
- Bookmark Folder
- Add Table
- Picture
- Language
- Text

To test if the code is well-formed, click **Compile**. To return to the last compilable code, click **Revert**.

> **Note:** Unless you have experience writing and editing code, Guidance Software recommends using default code in the report templates.

Editing Report Templates to Include Bookmark Folders in Reports

This section describes how to edit report templates to include bookmark folders in EnCase reports. Bookmarks are used in EnCase to store the data used in reports. The structure of the report is separate from the bookmarks’ folder structure. Using the report template for the report structure requires that you define the report to link bookmarks to the report sections.

The following examples assume that a bookmark folder structure exists and items have been added to the bookmark folders. The examples include both menu based customization and the use of ROC to modify reports.

Basic Report Section Editing and Formatting

1. On the home page, click **Report Templates**.
2. Select or create a report section to edit. You can use each report section to link bookmark folder items to the report and define the display format for those items.
3. In the **Options** tab, specify the name of the section.
4. Click the **Body Text** tab. This tab allows you to format text styles and layout of the bookmarks. You can also specify bookmark folder(s) for this section.
5. Click in the white space at the bottom of the report after the ROC word text and click **Bookmark Folder** from the toolbar. Selecting the **Show Folders** checkbox adds a heading based on the name of the folder. Click **Recursive** to start processing at the level selected and process all subfolders in the selected branch of that folder tree. To see the results of your selections, switch the lower View pane to **Report** for this section.
6. Select the **Formats** tab to set the formats for the bookmark items, such as **Folder, Note, Notable File, Text File, Data bookmark, Decode, Image, Record**, and **Email** types.
7. Double click or right click and select **Edit** to modify the detail presented for each of these bookmark types.

   For example, the default for an image bookmark is:

   ```
   style("Image") {image(width=2880, height=2880) par}
   ```

   You can modify this from the dropdown menus available to add Accessed, Created, and Written Times below the Image.

   ```
   style("Image") {
   image(width=2880, height=2880) par
   fieldname(field=Accessed) tab cell(field=Accessed)
   par
   fieldname(field=Created) tab cell(field=Created) par
   fieldname(field=Written) tab cell(field=Written) par
   ```

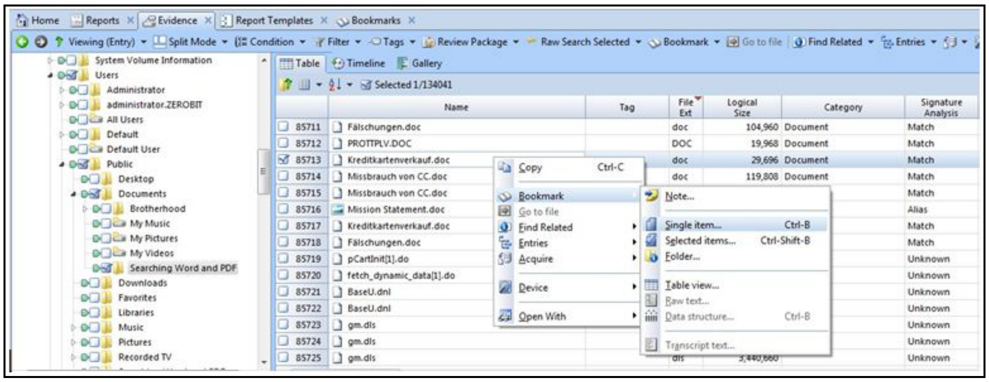
   You can see these changes in the View pane in the **Report** tab.

Editing the Report Template to Include the Item Path in Reports

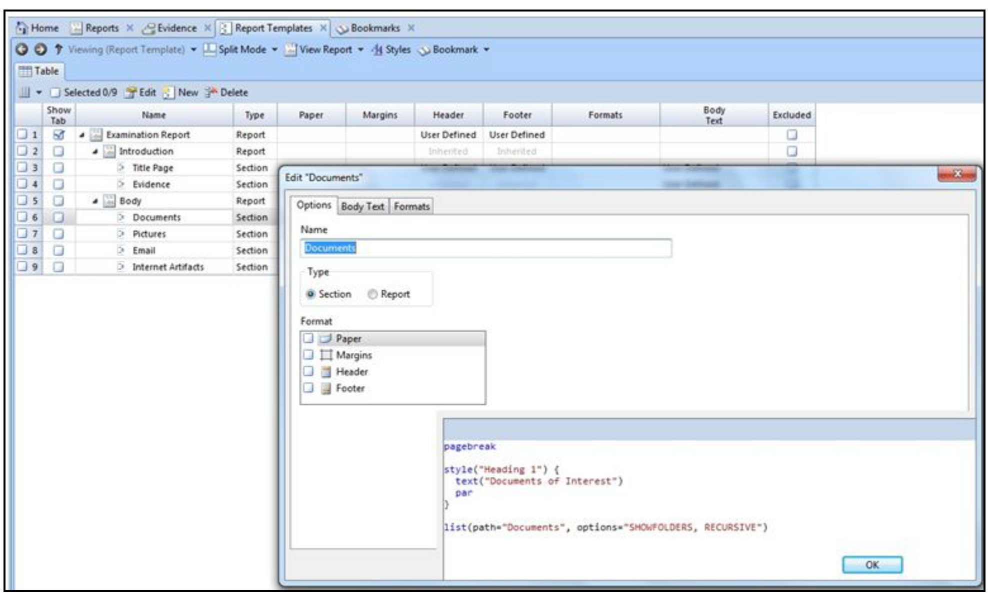
The following sections describe how to include the item path in reports based on documents and Internet artifacts.

BOOKMARKING DOCUMENTS AND DISPLAYING AN ITEM PATH

1. Bookmark your file to the required folder in your bookmark folder structure as a single item. If you have more than one item to bookmark, use **Bookmark** > **Selected items**. This example bookmarks relevant Documents into the Documents Folder.

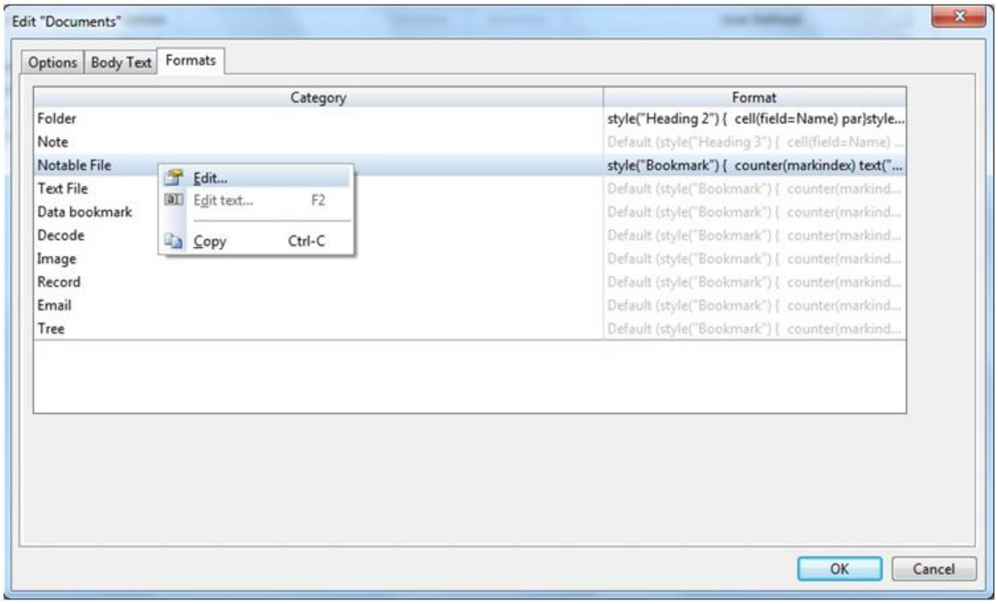


2. Open **Report Templates** from the EnCase Home screen or select **View** > **Report Templates**. Since the item to bookmark is in the Documents folder, this example shows how to edit the Documents Report Section to include the Item Path.

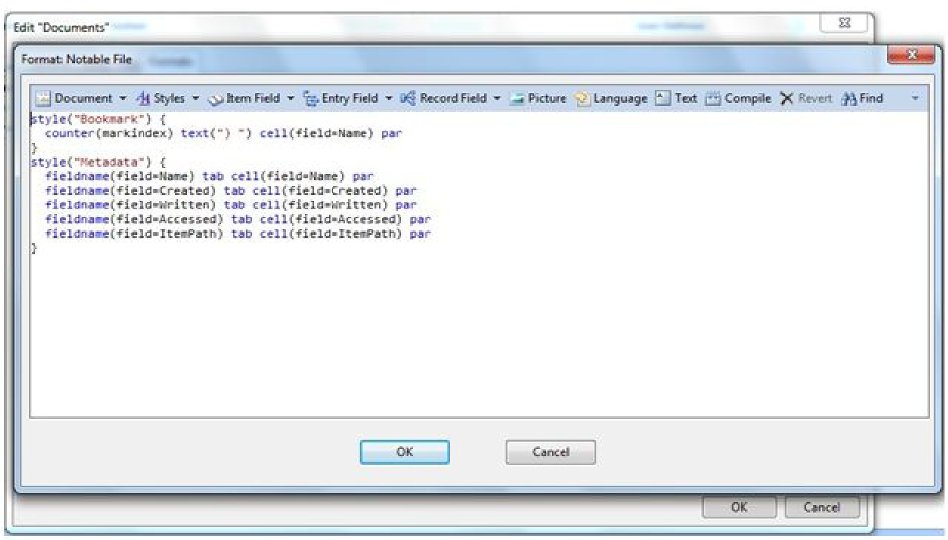


3. In the Edit Documents window, select the **Formats** tab. Select **Notable File** > **Edit**. Make sure the blinking cursor is positioned correctly, as the Item Path Field is added here. This

example shows the blinking cursor after the `fieldname(field=Accessed) tab cell (field=Accessed) par` statement.



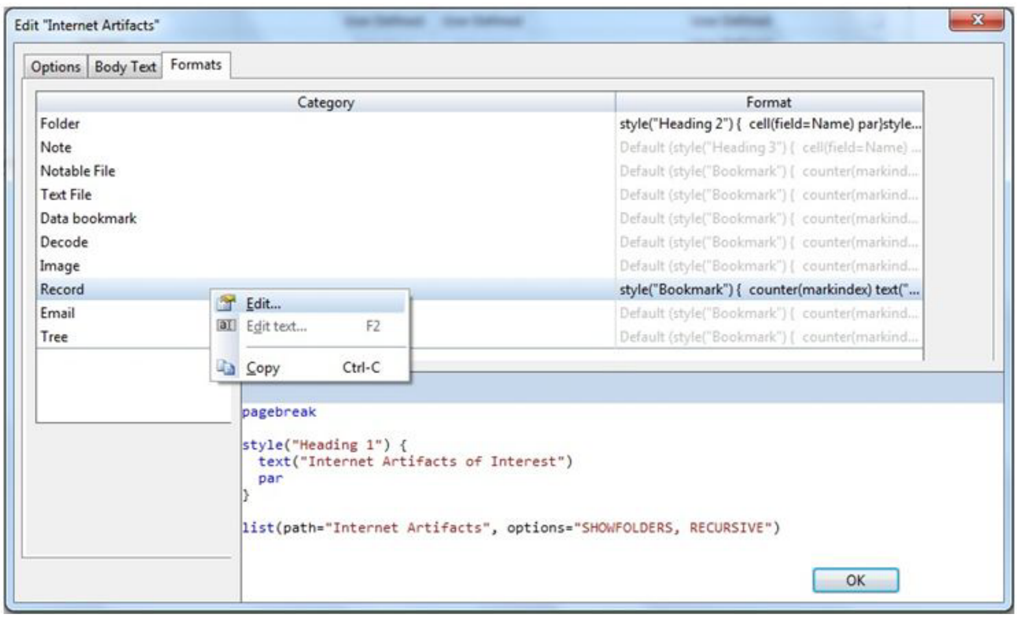
4. Drill down in the **Item Field** menu and select **Item Path**. `fieldname (field=ItemPath) tab cell(field=ItemPath)` displays on the last line. Adding `par` adds a line break in the report.
5. Click **OK** to exit **Report Templates**.



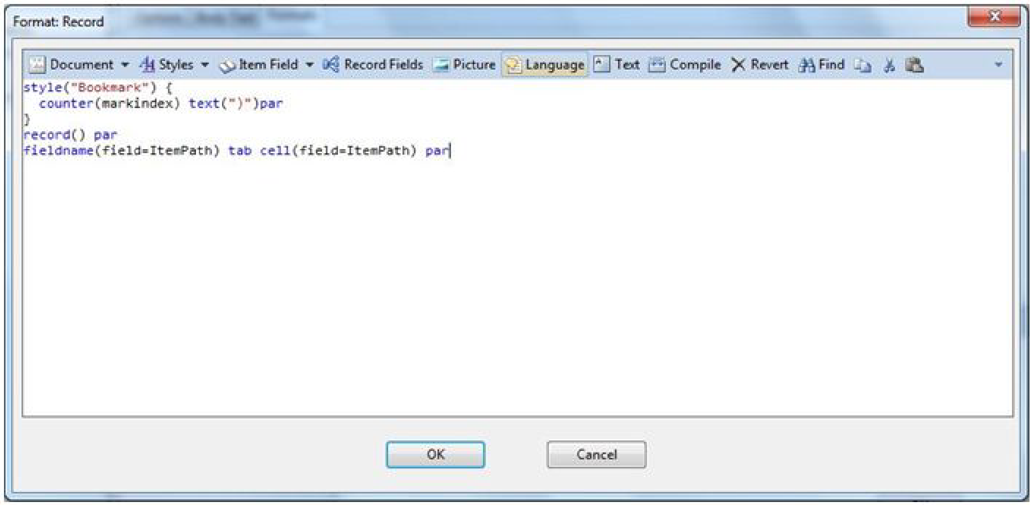
6. View your report. The Item Paths are added to the Document section of the report.

BOOKMARKING INTERNET ARTIFACTS AND DISPLAYING THE ITEM PATH ON REPORTS

1. Bookmark your file to the required folder in your bookmark folder structure as a single item. If you have more than one item to bookmark, use **Bookmark** > **Selected items**.
2. Open **Report Templates** from the EnCase Home screen or select **View** > **Report Templates**. Since the item to bookmark is in the Internet Artifacts Folder, edit the Internet Artifacts Report Section to include the Item Paths.
3. In the Edit Internet Artifacts window, select the **Formats** tab. Select **Record** > **Edit**. (Internet artifacts are Record data types.) Make sure the cursor is positioned correctly, as the Item Path Field is added here. This example positions the cursor after the `record () par` statement.



4. Drill down in the Item Field menu and select **Item Path**. `fieldname (field=ItemPath) tab cell(field=ItemPath)` displays on the last line. Adding `par` adds a line break in the report.
5. Click **OK** to exit **Report Templates**.



6. View the report. The Item Paths are added to the Internet Artifact section of the report.

Other than defining the specific report section to modify, the only difference in adding the Item Path field to the report is the category to be formatted. When adding Item Path to documents, the format category **Notable File** is being modified. When adding Item Path to Internet Artifacts, the format category **Record** is modified.

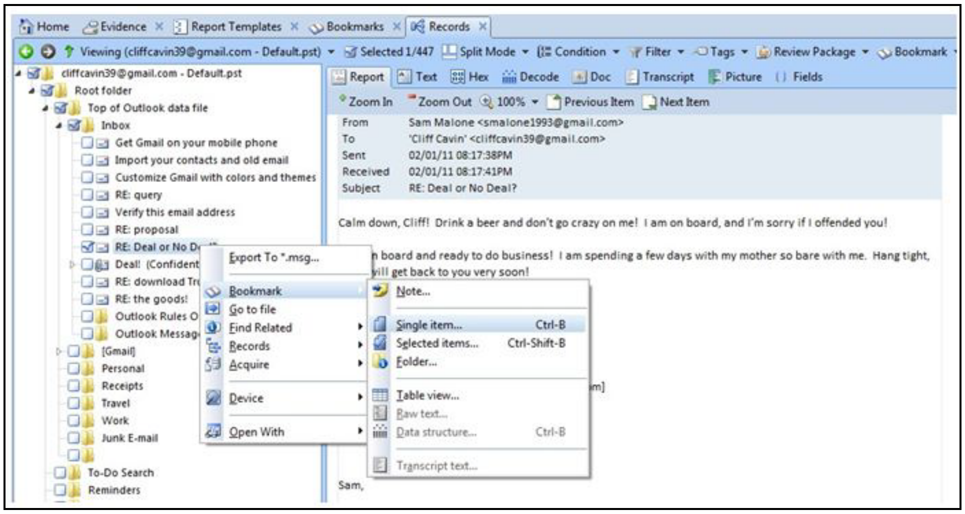
- Documents: Format **Notable File** category
- Internet Artifacts: Format **Record** category
- Pictures: Format **Image** category
- Emails: Format **Email** category

Editing the Report Template to Display Comments in Reports

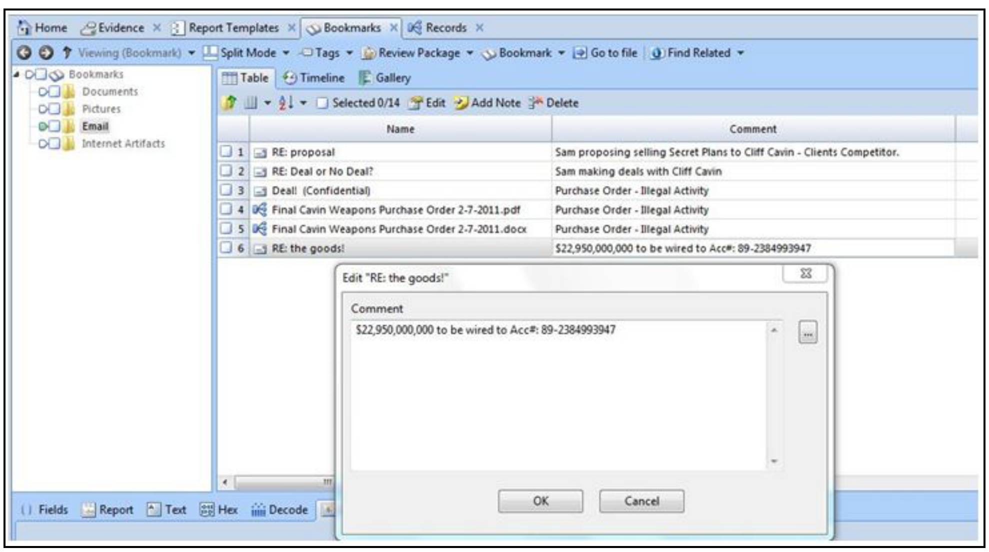
This section describes how to include comments in reports based on email bookmarks.

EDITING THE REPORT TEMPLATE TO BOOKMARK EMAIL AND DISPLAY COMMENTS IN REPORTS

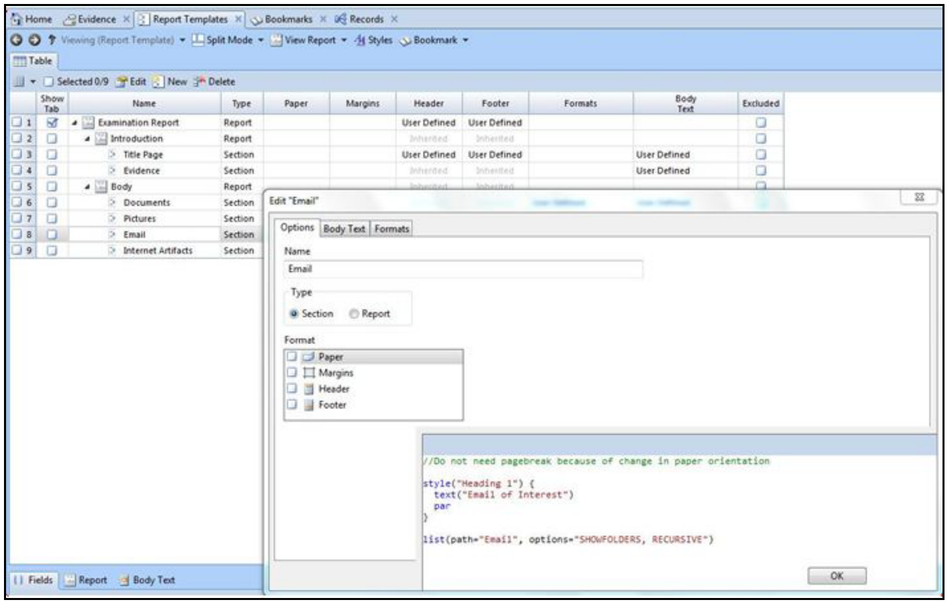
1. Bookmark your file to the required folder in your bookmark folder structure as a single item. If you have more than one item to bookmark, use **Bookmark** > **Selected items**. This example demonstrates bookmarking relevant Email into the Email Folder.



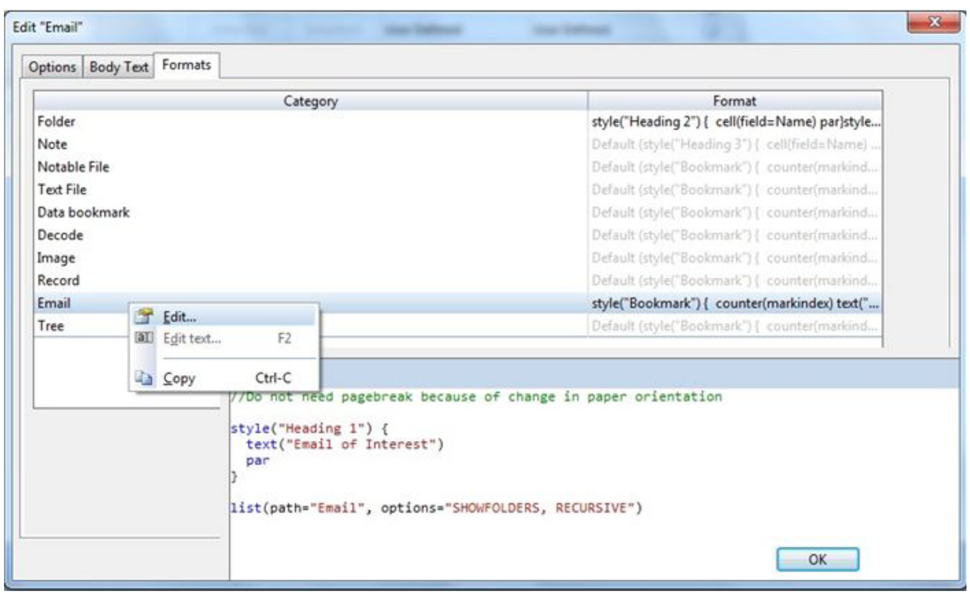
2. After bookmarking your entry, open the **Bookmarks** tab and locate the file. Add comments to your files by editing the Comment field. The comments made here are displayed in your report.



3. Click the **Report Templates** tab from the home page or select **View** > **Report Templates**. Since the item to bookmark is in the Email folder, edit the Email report section to include Comments.



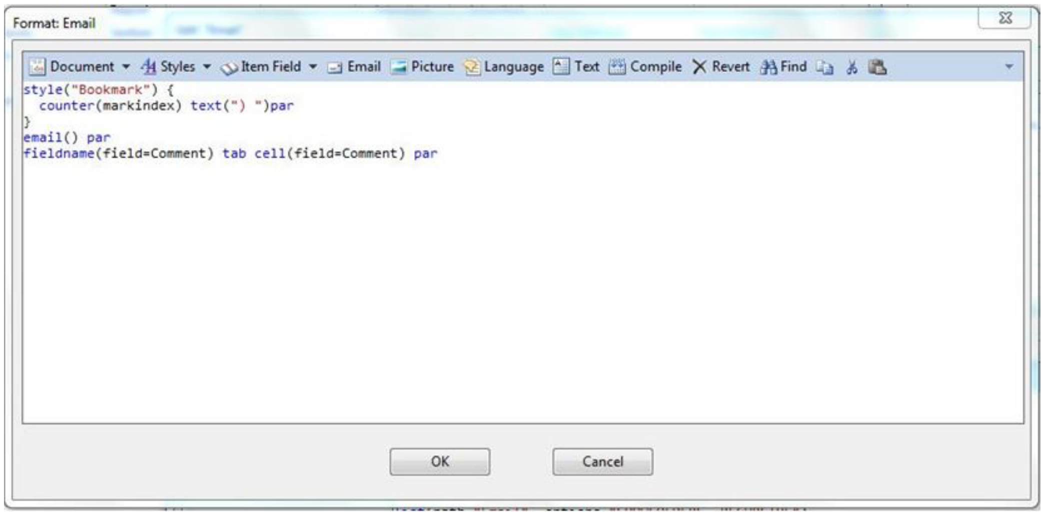
4. In the Edit Emails window, select the **Formats** tab. Select **Email** > **Edit**. Make sure the cursor is positioned correctly, as the Comment field is added here. In this example, the cursor is positioned after the `email () par` statement.



5. Drill down in the Item Field menu and select **Comment**. `fieldname(field=Comment) tab cell(field=Comment)` displays on the last line. Adding `par` adds a vertical line

spacing on the report.

6. Click **OK** to exit **Report Templates**.



7. View your report. Comments are added to the Email section of the report.

Report Object Code (ROC)

EnCase uses an optimized coding language called Report Object Code (ROC) which allows you to specify the format of pages and data content of reports. ROC describes the format of various Report Template components, including Header, Footer, Body Text and Formats. ROC is similar to other scripting languages, but is specifically designed for this purpose.

Guidance Software recommends that if you want to modify a report template or create your own, first refer to one of the supplied templates and read the examples in the following sections to see how ROC is structured and used.

Layout Elements

The following is a complete list of all ROC layout elements. These elements are also available from the menus in the Edit window.

Element	Definition and Usage
par	Inserts a line break.
space	Inserts a space.

Element	Definition and Usage
tab	Inserts a tab.
pagebreak	Inserts a page break.
pagenumbe r	Inserts a page number.
hline	Inserts a horizontal line. Example: `hline(height=x)` **height** is the height of line expressed in twips (twentieth of a point)
currentdate	Inserts the current date at time the report is generated.
text	Inserts static text. Example: `text("My text goes here.")`
lang	Displays a predefined string in the language of the EnCase version that is running. Example: `lang(x)` The parameter is the ID of the string to display

Element	Definition and Usage
image	Displays an image from a path on the filesystem. Example: `image (path="C:\\Users\\user.name\\Pictures\\EnCase_big.bmp", width=760, height=400)` **path** is the path of the image **width** and **height** are numbers that express the width and height of the image in twips
hyperlink	Inserts a hyperlink to a web location. Example: `hyperlink("http://www.link.com") { text ("Hyperlink") }` **hyperlink** is the link destination **text** is the text that displays in the report
style	Defines the style to apply to the elements within the style block. Example: `style("Footer Heading") { // content here }` **style** is the name of the style The content inside the braces displays according to the style.

Content Display Elements

Element	Definition and Usage
list	Displays all bookmarks in the specified path according to the format of the bookmark as defined within the section. Example: `list (path="Examination\\Report\\Introduction", options="RECURSIVE, SHOWFOLDERS")` **path**: bookmark folder containing the bookmarks to display (required) **options**: • RECURSIVE: Display all items within all subfolders in that folder. • SHOWFOLDERS: Display the folder name before displaying the contents of a subfolder • If you select no options, only the bookmarked items in the specified folder display.

<table>
<tr><th>Element</th><th>Definition and Usage</th></tr>
<tr><td>table</td><td>Displays a table of items of the specified type.

Example:

<code>table(type=CaseInfo, options="SHOWTABLE, SHOWBORDER", columns="Name,Value")</code>

type: DataType to display in the table (required).

columns: The columns to display in the table. All columns display if column values are not defined (optional).

options:
SHOWTABLE: Display the items in a table where each item has one row, and the fields are displayed in columns.
SHOWBORDER: Display a border on the table.
SHOWHEADER: Display column names in a header row.
SHOWICONS: Display the icon associated with the name field.
SHOWROWS: Display the number of each row.
SHOWALL: Combine all display options.</td></tr>
</table>

Element	Definition and Usage
cell	Displays the content of a particular field. Example: `cell(type=CaseInfo, node="Case Number", field=value,  options="PAR")` **type**: DataType to display in the cell (optional). Valid types for use in body text and formats: LogRecord, Bookmark, Evidence, CaseInfo. **node**: The name of the node to be displayed (optional). field: the field to display **options**: • PAR: Add paragraph only if text exists.

Element	Definition and Usage
fieldname	Displays the name of a particular field. Example: `fieldname(type=Case, field=value, options="PAR")` **type**: DataType to display in the cell (optional). Valid types for use in body text : LogRecord, Bookmark, Evidence, CaseInfo. Valid types for use in formats: Case, Bookmark, Record, Entry. **field**: the field to display **options**: • PAR: Add paragraph only if text exists.
data	Inserts the contents of a Table view bookmark. `data()`
artifact	Inserts the contents of a Notable File bookmark of a non-email artifact (for example, Internet History). `artifact(fields="<comma-delimited list of fields>")` **fields**: Fields to display in the artifact (optional)
email	Inserts the contents of a Notable File bookmark of an email artifact. Example: `email(fields="<comma-delimited list of fields>")` **fields**: Fields to display in the email (optional).

Element	Definition and Usage
folder	Inserts the contents of a Folder bookmark. `folder()`
image	Displays a bookmarked image. `image(width=1440, height=1440)` **width**: width of the image, in twips **height**: height of the image, in twips
filelink	Inserts a link to a file. Example: `filelink() { cell(field=Name) }` The text inside the braces displays as the link.
counter	Inserts an incremental count for the item. Example: `counter(<name>)` The parameter is the name for this counter.
doctitle	Displays the name of the case.
docpath	Displays the path of the case.

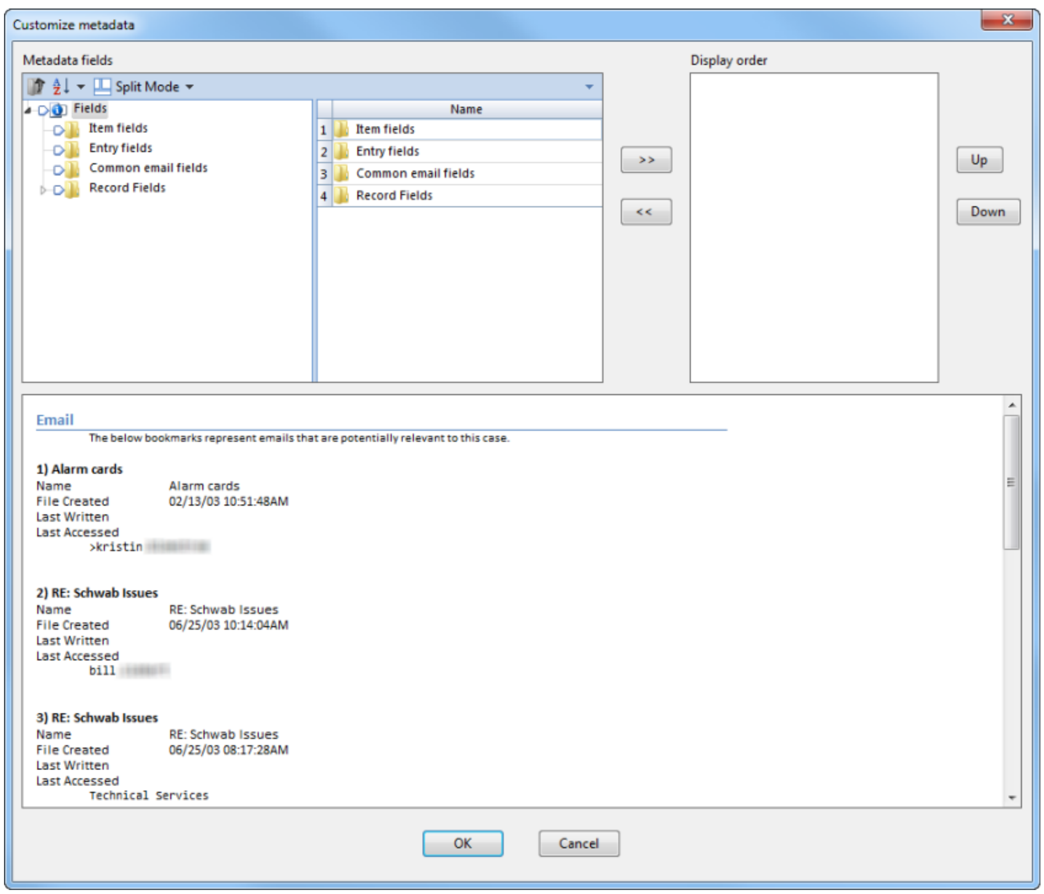
Report Template Wizard

You can access reports directly and add folders to a report by using the Report Template Wizard.

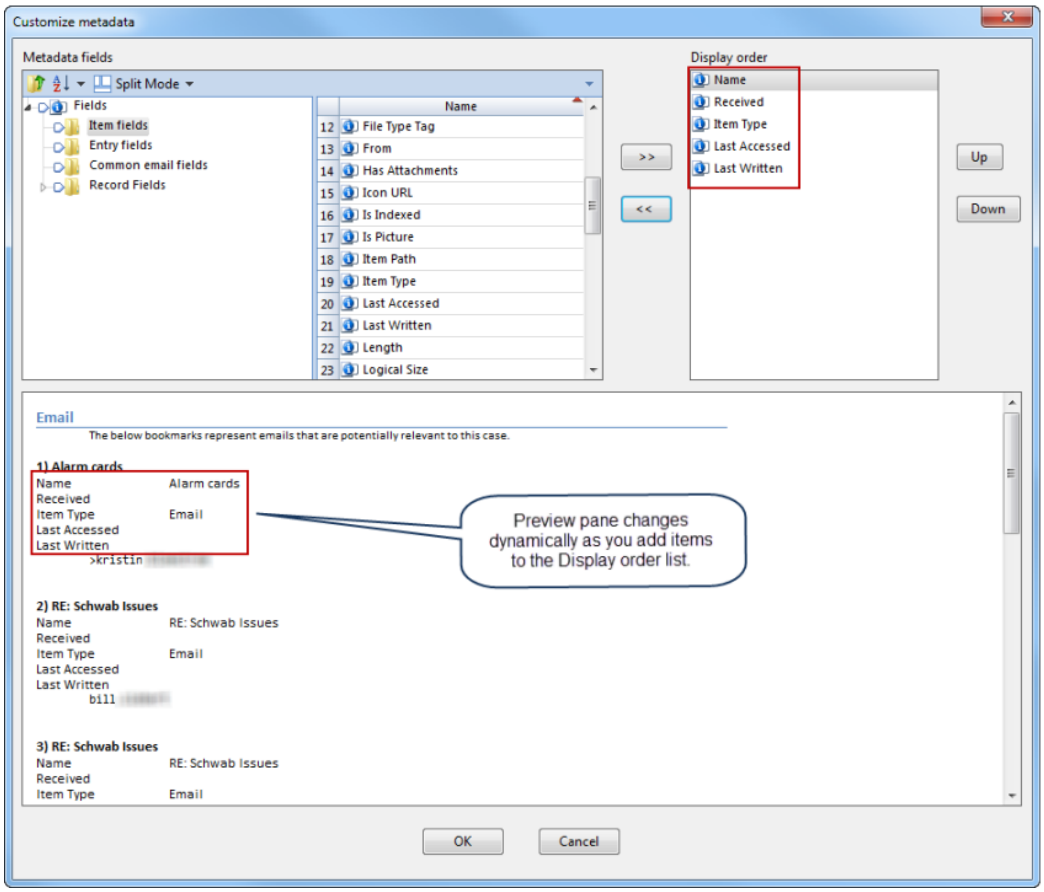
Connecting Bookmark Folders and Report Sections

To use the report template wizard:

1. On the **Bookmarks** tab, click **Reports**, then click **Add folder to report** from the dropdown menu.
2. The Add folder to report dialog displays.
3. Select an existing section, or create a new custom section. To create a new section, enter a section name in the <New Section Name> area and click **Add**. The new section is created as a child of the currently selected section or report.
4. Click **Next**. The second Add folder to report dialog displays. It enables you to apply commonly used formatting to the report. When you click a Report section formatting checkbox, the wizard generates Report Object Code automatically.
    - **Restart numbering** restarts numbering at 1 in a new section, instead of continuing numbering from a previous section.
    - **Hyperlink to exported items** configures the report section to add a hyperlink to exported data.
5. Click **Preview** to see how the formatting will display in the report.
6. To add metadata, click **Customize metadata**. The Customize metadata dialog displays.



- In the Metadata fields pane on the left, click the field you want to work with (Item fields, Entry fields, Common email fields, Record fields).
- In the Name pane in the middle, click the name of a metadata type you want to add to the report, then click the double right arrow button (**>>**) to add it to the Display order list.
  - Note that as you add metadata items to the Display order list, the preview pane updates dynamically to reflect your choices.

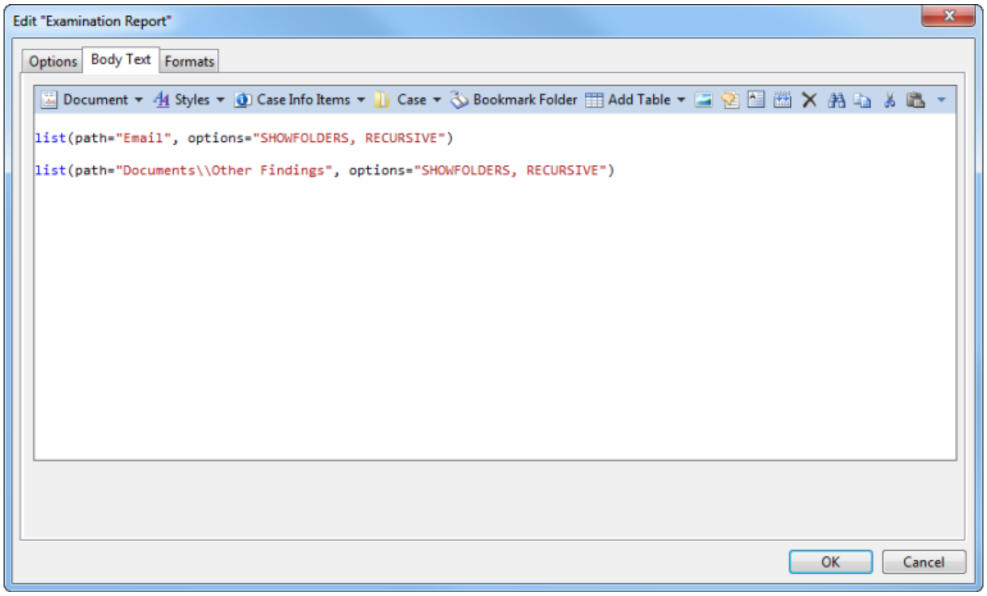


- To change the order, click the item in the Display order list you want to change, then click the **Up** or **Down** button. Repeat as necessary to get the order you want.
- To remove an item from the Display order list, click it, then click the double left arrow button (**<<**).

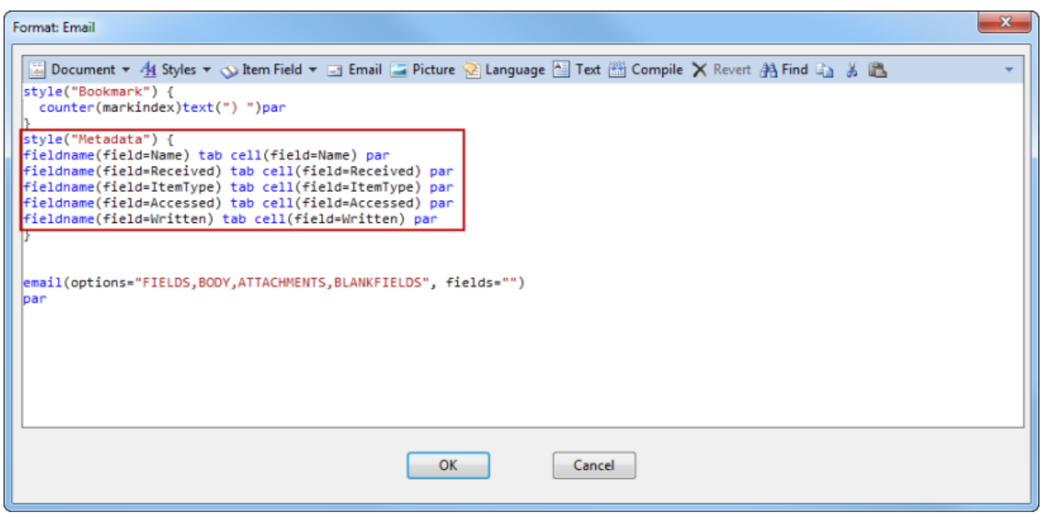
7. When finished, click **OK**.
8. Back in the Add folder to report dialog, click **Finish**.

You can view the Report Object Code that the Report Template Wizard added to the template.

In this example, bookmarks folders were added to "Examination Report":



In this example, formats were updated with specified metadata:



Hiding Empty Report Sections

You can hide sections that do not contain any bookmarks.

1. On the **Bookmarks** tab, click **Reports** > **View Report**, then click the report you want to view.
2. The report displays. Click the **Hide empty sections** checkbox. Any empty sections no longer display in the report.

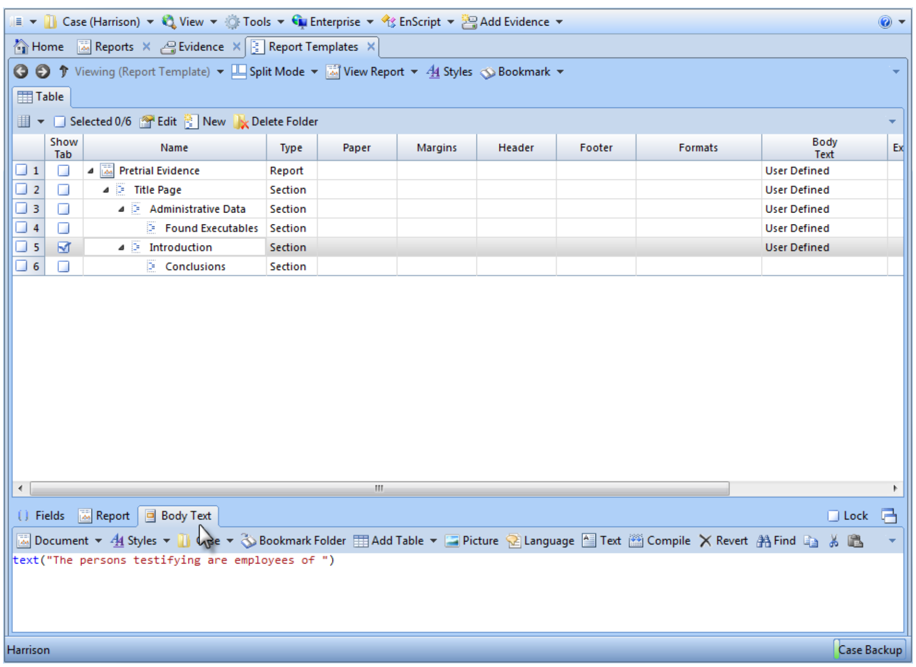
Creating Hyperlinks to an Exported Item from Report Templates

You can embed hyperlinks and link to exported files. The ways to do this are described below.

Using Bookmarks to Link to an External File

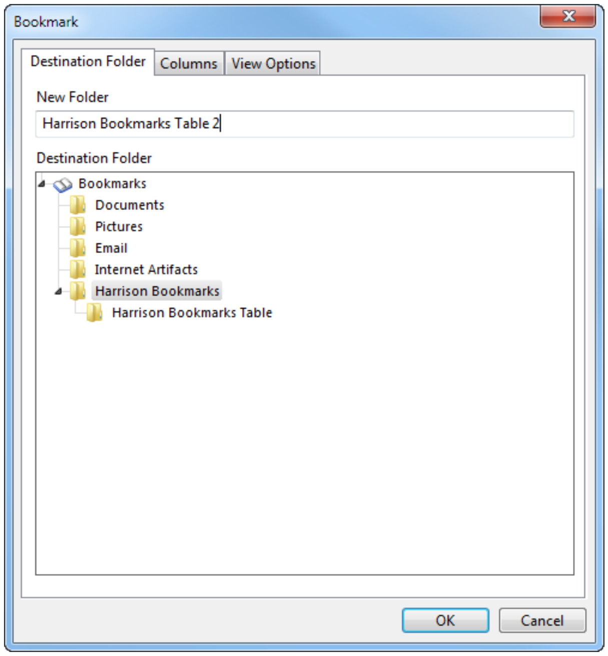
To select and display bookmarks in a report:

1. In Report Templates view, check the part of the report where you want the bookmarks to display, then click the **Body Text** tab in the lower pane.

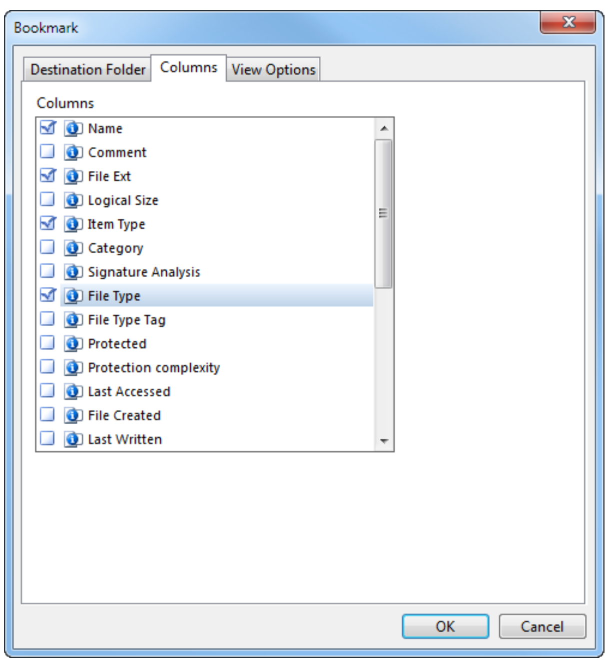


2. In the Add Table dropdown menu, click **Bookmark Folder**.

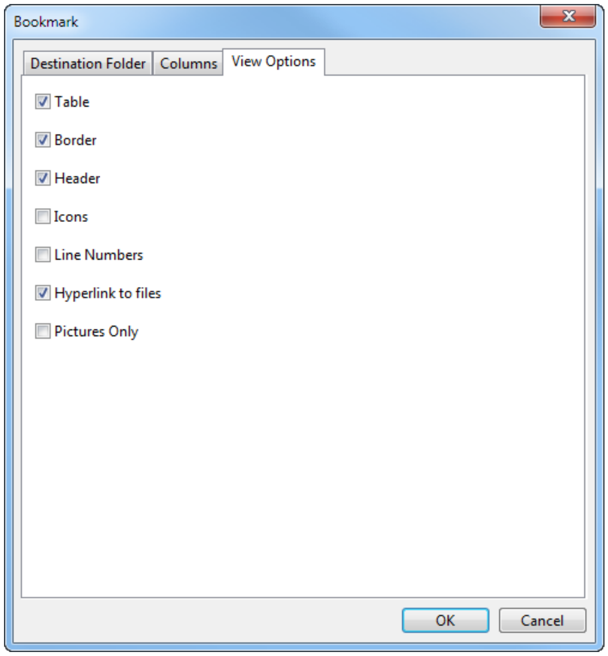
3. The Bookmark dialog displays.



4. In the **Destination Folder** tab, select the folder where you want the table to be saved and enter a folder name.
5. In the **Columns** tab, click the checkboxes for the columns you want to display in the table.



6. In the **View Options** tab, click the checkboxes for the options you want. Be sure to click the **Hyperlink to files** checkbox.



7. Click **OK**. The bookmarks display as hyperlinks in the table in the report.

Exporting a Report to Display Hyperlinks

To export a report to display hyperlinks:

1. Right click, then click **Save As** from the dropdown menu. The Save As dialog displays.
2. For the Output Format, select **RTF**, **HTML**, or **PDF**, then click the **Export items** checkbox.

   Note: The Export items checkbox is disabled for the other formats.

3. Accept the default path or enter another path. If you want to view the exported report after saving, click the **Open file** checkbox.
4. Click **OK**. The hyperlinks display in the exported report.

Exporting a Metadata Report to Display Hyperlinks

To display hyperlinks in a metadata report:

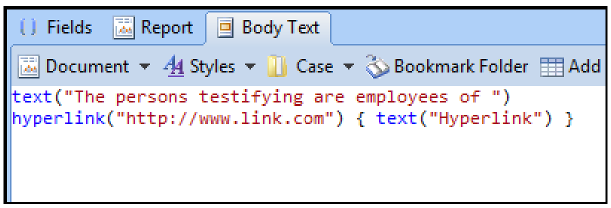
1. In the **Evidence** tab, select the item you want to display as a hyperlink in the report.
2. In the lower pane, click the **Report** tab to display metadata.
3. Right click and select **Save As** from the dropdown menu. The Save As dialog displays.
4. Select the Output Format you want. The supported formats are RTF, HTML, and PDF.

5. Click the **Export items** checkbox. If you want to view the report after saving, click the **Open file** checkbox.
6. Accept the default path, or enter a path of your own, then click **OK**.
7. The hyperlink displays in the metadata report.

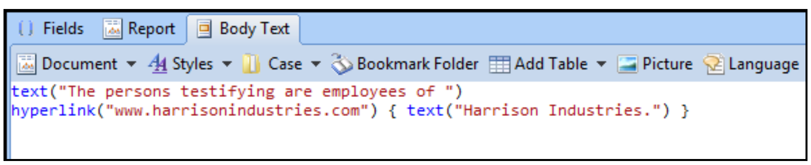
Adding a Hyperlink to a URL

To add a hyperlink to a URL:

1. Go to Report Templates view. Select the part of the report where you want to add a hyperlink, then click the **Body Text** tab in the lower pane to display the text.
2. Place the cursor where you want to insert the hyperlink, then click **Hyperlink** in the Document dropdown menu.
3. A line of hyperlink code displays.



4. Replace http://www.link.com with the URL for your hyperlink. Replace Hyperlink with the text you want to display for the hyperlink.



5. Save your work. The hyperlink displays in blue in the report.

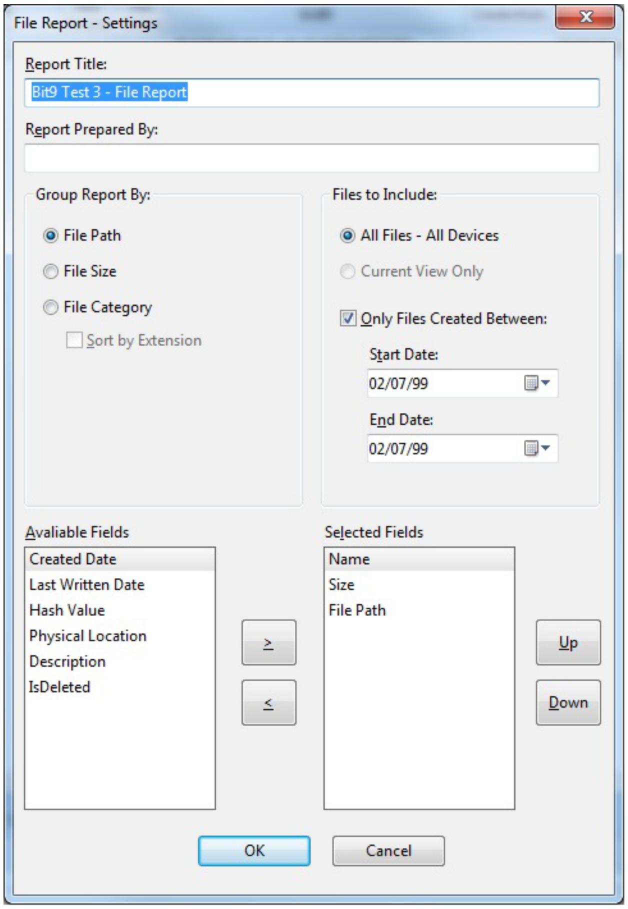
File Report EnScript

The File Report EnScript is a standalone script that produces a file listing that includes file metadata. You can select which device to run the script against and set the following report information:

- Report name
- Examiner
- Grouping results
- All files or specified files
- Display fields

Running the File Report EnScript

1. From the EnScript menu, select **File Report**. The File Report - Settings dialog displays.



2. In the Report Title field, enter the name of the report. The default report title format is [Case Name] - File Report.
3. In the Report Prepared By field, enter the name of the examiner. The default examiner name is drawn from the specified examiner in Case Info.
4. On the left side of the dialog, specify how you want to group your report.
   - **File Path** sorts files by the file system's location of each file, sorted according to Item Path.
   - **File Size** sorts files according to size in Kilobytes.

- **File Category** sorts files alphabetically, according to file category. To sort by the three-character file extension within a category, click the **Sort by Extension** check-box.

5. On the right side of the dialog, specify whether to include all files, only files in the current view, and/or files created within a specified range. To specify a creation date range:
   - Select the checkbox for **Only Files Created Between**.
   - Enter the Start Date directly, or click the calendar browser button.
   - Enter the End Date directly, or click the calendar browser button.

6. At the bottom of the dialog, use the field selector to include/exclude and order the fields for your report.
   - In the Available fields box on the left, select any field you want to include in your report and click the right arrow.
   - In the Selected fields box on the right, select any field you want to exclude from your report and click the left arrow.

7. To order the selected fields for your report, select each field and move it with the **Up** or **Down** buttons.
8. Click **OK**. The File Report EnScript generates the file report, and it displays in the File Report window.

Saving the File Report

1. After verifying the content of the report, right click the report and select **Save As...**. The Save As dialog displays.
2. Select the output format.
3. Specify a path for the output. To browse your file system, click the ellipsis button.
4. To open the report in the selected output format, select the **Open file** checkbox.
5. Click **OK**. If you selected the **Open file** checkbox, the file opens in the selected output format.

Viewing a Report

To view a report:

1. In the **Report Templates** tab, click **View Report** from the tab toolbar. The dropdown menu lists all reports that have the **Show Tab** option set.
2. Select the report you want to see. The report displays in the viewer.

To save a report, right click on the report and select **Save As**.

The following output formats are available:

- TEXT
- RTF
- HTML
- XML
- PDF

Once you select the output format, specify a Path and optionally set the **Open file** option if you want the file to open in the default application after saving.

> **Note:** To edit a report in Microsoft Word, save the report in RTF format. The EnCase RTF report is fully compatible with Microsoft Word.

CHAPTER 14

ACQUIRING MOBILE DATA

Overview	433
Acquiring Mobile Device Data (General Process Description)	435
Acquiring Data from iPhones/iPods/iPads/iPod Touches	439
Acquiring Data from Android OS Devices (Including Kindle Fire Tablets and Android Wear)	465
Acquiring Data from Tizen Devices	486
Acquiring Data from RIM BlackBerry Devices	488
Acquiring Data from Symbian OS Smartphones	491
Acquiring Data from a WebOS Based Device	510
Acquiring Data from PDAs	513
Acquiring Data from GPS Devices	534
Acquiring Data from Feature Phones	547
Acquiring Data from SIM Cards	584
Acquiring Data from Memory Cards/Mass Storages/e-Readers/Portable Devices	589
Importing Data	592
Importing Cloud Data	598

Overview

EnCase can acquire a variety of mobile devices, including smartphones, tablets, PDAs, and GPS navigation devices. Additionally, you can import mobile device backup files and Cellebrite UFED case files. You can also acquire data from cloud services, such as Facebook, Twitter, Gmail, and Google Drive.

Acquired or imported mobile data is saved as an EnCase Logical Evidence File in the folder you specify in the Output File Settings.

Before beginning acquisition on a mobile device, you will need to download and install the Mobile Driver Pack from the Guidance Software Download Center.

> **Note:** If you are running Windows 7, you will need to install two security updates before you can install the Mobile Driver Pack. Windows 7 needs to be upgraded to SP1 before installing the security updates.

Installing the Mobile Driver Pack

Before beginning acquisition on a mobile device, you will need to download and install the Mobile Driver Pack.

> **Note:** If you are running Windows 7, you will need to install two security updates before you can install the Mobile Driver Pack. Windows 7 needs to be upgraded to SP1 before installing the security updates.

To install the Mobile Driver Pack:

1. Download the Mobile Driver Pack.
2. Double click on EnCaseMobileDriverPack1.0Setup.exe to launch the installer.
3. Click **Next**.
4. Accept the License Agreement and click **Next**.
5. On the Customize Setup screen, leave Drivers and Tools set to **Will be installed on the local hard drive**. Click **Next**.
6. Click **Install**.
7. Click **Finish** after the installation completes.

Types of Data Acquisition

The acquisition methods used to extract data from a device include logical and physical acquisition. For most devices, both of these acquisition types are available. For others, only one type of acquisition is available.

The process of data acquisition completely depends on the type of device.

During the Logical Acquisition Process, the program uses the commands and protocols that allow you to work with the device using its own OS. This means that each device has some commands that allow it to exchange data with the PC by the means of some simple protocols (i.e., the AT protocol).

Due to this, you can acquire only data designed by the OS to be passed using the protocol. But the main part of the data will be completely parsed and shown in a readable format.

During the Physical Acquisition Process, the program doesn't use commands of the device's OS. Usually, a special program is written into the device memory (into a part where data is not stored). A complete memory image is acquired and all data is extracted from it if possible.

In this case, the data is usually not parsed but the required information can be found in it anyway.

> **Note:** During acquisition, the data on the device cannot be damaged or lost and its structure and content do not change.

Data Parsing

Data Parsing is the process of decoding information and displaying it in a human-readable form for analysis and reporting.

Data parsing is usually done automatically for any type of data that can be parsed.

> **Note:** Not all types of data can be parsed and not all plug-ins contain parsers. For more information, see the description of each plug-in.

Acquiring Data from Different Devices

In most cases, the logical and physical data acquisition methods are available for each supported manufacturer.

For most plug-ins, data acquisition is performed using the standard process and does not include any additional interaction with the devices. For some plug-ins, however, the acquisition process requires some additional steps.

The data acquisition process differs from the general process for the following types of devices:

- Android OS Devices
- Advanced Android LG Devices
- Garmin GPS
- iPhone/iPad/iPod Touch
- Motorola
- Motorola iDEN
- Nokia Symbian OS
- Palm OS Based Devices
- Psion 16/32 Bit Devices
- RIM BlackBerry
- Samsung GSM
- Siemens
- SIM Card Readers
- Symbian 6.1 Devices
- Tizen Devices
- WebOS Based Devices
- Windows Mobile Devices

It is highly recommended that you read the instructions for each of these devices before you start acquisition.

Acquiring Mobile Device Data (General Process Description)

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

There are two methods of device detection: **automatic detection** and **manual plug-in selection**.

- **Acquisition via automatic detection:** This method automatically detects the devices connected to the computer via a USB port and allows you to select the type of acquisition of the device.
- **Acquisition via manual plug-in selection:** This method allows you to select a plug-in corresponding to the device manufacturer and acquisition type as well as the connection via which acquisition will be performed.

Guidance Software recommends acquiring via automatic detection. Use manual plug-in selection only in the event that the device is not detected or cannot be acquired via automatic detection.

Data acquisition usually consists of the following steps:

1. **Preparation Step:** Prepare the device for working with the program. Guidance Software recommends the following:
   - Check whether the device is charged in order to prevent power loss during the acquisition process.

     Note: Acquisition from PDAs, iPhones, and Androids might take several hours.

   - Choose the proper cable or cradle for your device.
   - Ensure the proper drivers for any USB cable (cradle) are installed.
   - Check that the device is connected to the computer.
   - Insert or remove the SIM card depending on the requirements of the plug-in you are using and your procedures.
   - Turn the device on or off depending on the requirements of the plug-in you are using.
   - If acquisition of the device is NOT being performed for the first time within this case, it is recommended that you reload (power cycle) the device before starting the new acquisition process.

2. **Selection Step:** Go to **Add Evidence > Acquire Mobile > Acquire from Device** to start the Acquisition Wizard, which will guide you through the process of acquisition. The following items must be selected:
   - **For automatic detection:**
     - The device whose data you want to acquire.
     - The type of acquisition you want to perform.

   - **For manual plug-in selection**
     - The manufacturer and type of acquisition (see the list of acquired data for the corresponding device for the differences between the amount and type of data acquired with the logical and physical acquisition methods).
     - The model of your device (most of the plug-ins allow the program to detect the model automatically).
     - Type of connection (the port to which the device is connected).

3. **Instructions Step:** You can read special acquisition instructions if they are available for the selected device.
4. **Acquisition Step:** The program acquires information from the device. In some cases, you might need to perform more actions with the device, such as pressing special buttons on it or entering special information. The process of acquiring the device features is displayed in the progress table.
5. **Final Step:** Acquisition finishes, and you can disconnect your device from the computer.

There can be certain specifics about acquisition of different types of devices. For more information, see the description of data acquisition of the type of device you want to acquire.

> **Note:** The program allows you to work with other data in the case during the acquisition. You can add, view, and process other evidence in the case while the device is being acquired.

Acquisition via Automatic Device Detection

To acquire a device via automatic detection:

1. Turn on the device.
2. Check that the device is fully charged.
3. Connect the device to the computer with a data cable. If a USB connection is used, check that the proper drivers are installed.

   > **Note:** If you use the dongle version of the program, shut down the program and unplug your dongle before installing the drivers. Please note that installing drivers without unplugging the dongle can damage it.

4. In EnCase Forensic , select **Add Evidence > Acquire Mobile > Acquire from Device**.
5. On the Acquisition Wizard Welcome screen, an icon representing your device will be displayed. Click the icon of your device. If your device is not displayed, click the troubleshooting link in the bottom of the page.

   > **Note:** Guidance Software recommends working with only one connected device at a time.

6. On the **Acquisition Type** page, select the type of acquisition you would like to perform.

   > **Note:** Physical acquisition of some devices, such as CDMA and Siemens devices, can only be performed via manual plug-in selection.

7. If you selected **Custom Logical Acquisition**, on the **Feature Selection** page, select the features you want to acquire from the device and click **Start Acquisition**.

8. Data acquisition starts, and its progress is displayed on the Acquisition Progress page.

   Note: The program allows you to work with other data in the case during the acquisition. You can add, view, and process other evidence in the case while the device is being acquired.

9. When data acquisition finishes, the case is saved. Click **Finish**.

   Note: This process may take some time.

10. Disconnect your device from the computer.

Acquisition via Manual Plug-in Selection

To acquire a device via manual plug-in selection:

1. Turn on the device.

   Note: Samsung and Siemens cell phones must be turned off before performing physical acquisition.

2. Check that the device is fully charged.
3. Connect the device to the computer with a data cable. If a USB connection is used, check that the proper drivers are installed.

   Note: If you use the dongle version of the program, shut down the program and unplug your dongle before installing the drivers. Please note that installing drivers without unplugging the dongle can damage it.

4. In EnCase Forensic Endpoint Investigator, go to **Add Evidence > Acquire Mobile > Acquire from Device**.
5. On the Acquisition Wizard Welcome page, click **Manual plug-in selection**.
6. On the Plug-in Selection page, select the plug-in corresponding to the device manufacturer and the type of acquisition you want to perform and click **Continue**.
7. On the Connection Selection page, select the port to which the device is connected. Click **Start Acquisition**.

   Note: For some device types, like Samsung GSM, Siemens, and Psion 16/32-bit devices, you will need to select a model of the device.

8. Data acquisition starts, and its process is displayed on the Acquisition Progress page. On this page, you can see which features have been successfully acquired and which features have not and why.

Note: The program allows you to work with other data in the case during the acquisition. You can add, view, and process other evidence in the case while the device is being acquired.

9. When data acquisition finishes, the case is saved. Click **Finish**.

   Note: This process may take some time.

10. Disconnect your device from the computer.

   Note: The data acquisition process will be different for some devices. For more information, see the description of data acquisition of the type of device you want to acquire.

Acquiring Data from iPhones/iPods/iPads/iPod Touches

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

About Data Acquisition of iPhones/iPods/iPads/iPod Touches

The program allows you to acquire information from iPhones, iPods, iPads, and iPod Touches.

You can perform the following types of acquisition:

- **Logical acquisition of iPhone/iPad/iPod Touch devices:** Logical acquisition of iPhone/iPad/iPod Touch devices is performed via the **iPhone/iPad/iPod Touch Advanced logical plug-in**, which allows you to acquire a backup and application data of any version of iPhones, iPads, and iPod Touches. Acquired data will be partially parsed.
- **Physical acquisition of iPhone/iPad/iPod Touch devices:** Physical acquisition of iPhone/iPad/iPod Touch devices is performed via the **iPhone/iPad/iPod Touch physical plug-in**. Acquired data will be partially parsed.

  Note: To acquire a non-jailbroken iPhone/iPad/iPod Touch device physically, you must first put the device into the DFU mode.

- **Physical acquisition of iPod devices:** Physical acquisition of iPod devices is performed via the **iPod physical plug-in**.

iOS Logical Acquisition

> **Note:** For devices running iOS 7 and later, a message that reads **Do you trust this computer?** appears on the device when it is plugged into a computer. Tap **Trust** to establish a trusted connection before beginning acquisition.

Data acquisition is performed using the standard process.

Logical acquisition is performed via the **iPhone/iPad/iPod Touch Advanced Logical Plug-in**.

iOS Physical Acquisition

If your device is non-jailbroken, you need to put it into Device Firmware Upgrade (DFU) mode before acquisition. DFU mode allows all devices to be restored from any state. Please note that no data will be damaged or lost after putting the device into DFU mode.

Data acquisition is performed using the standard process.

> **Note:** Devices running iOS 8.4 may be acquired only after being jailbroken via the TaiG jailbreak. For more information, visit http://www.taig.com/en/.

Physical acquisition is performed via the **iPhone/iPad/iPod Touch Physical Plug-in**.

To put the device into DFU mode:

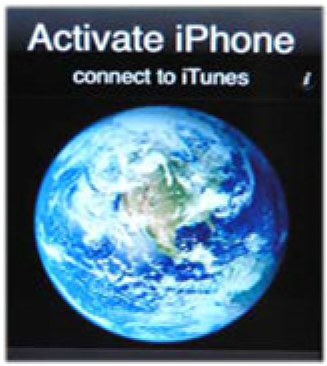
1. Plug the device into your computer.
2. Turn off the device.
3. Hold the **Power** button for 3 seconds.
4. Hold the **Home** button without releasing the **Power** button for 10 seconds.
5. Release the **Power** button, but keep holding the **Home** button.
6. Keep holding the **Home** button until your device screen becomes completely blank (for about 15 seconds). Please note, if a device in the DFU mode is being connected to the PC for the first time, the driver installation will automatically start.
7. Make sure the device screen is blank and no logos are present.
8. When acquisition finishes, exit the DFU mode on your device. To do this, hold the **Home** and **Power** buttons until the Apple Logo appears.

iPhone Reaction during Acquisition

During the acquisition process of a jailbroken device, the iPhone goes through several states in which it shows different messages on the screen.

It may look like this:

1. Connection step:
   a. Normal mode (that is what the device looks like before the connection starts)



   b. Recovery mode



> **Note:** At this stage, the device requires a connection to iTunes. The program establishes this connection. Do not connect to iTunes manually.

   c. Restore mode (switching between two modes)



d. Normal mode



e. Recovery mode



f. Restore mode



2. Acquisition step:

Note: For devices running iOS 7 and later, a message that reads **Do you trust this computer?** appears on the device when it is plugged into a computer. Tap **Trust** to establish a trusted connection before beginning acquisition.



3. Disconnection step:
    a. Recovery mode



    b. Normal mode (the device has returned to its default state)



Acquired Data - iPhone/iPad/iPod Touch

Logical acquisition of iPhone/iPad/iPod Touch devices allows you to acquire the following groups of data, both from standard and jailbroken devices, using internal Apple protocols:

- Parsed data
- Deleted parsed data in binary files (including Address Book, Calendar, Call History, iMessages, Network Connection, Email messages, Notes, Safari Bookmarks, Messages, and SMS Search)
- File system in binary files
- Device properties
- Backups made from iOS 11 devices

Note: Device properties are acquired only from devices with iOS 5.x and higher.

Usually the amount of acquired data depends on the model and state of the phone.

Note: The file system is acquired only partially, e.g., it does not contain system files of the iPhone.

The following types of data are acquired from iOS devices:

Data Type	Standard Devices	Jailbroken Devices
Parsed data		
Contacts	✓	✓
Messages	✓	✓
Call history	✓	✓
iMessages	✓	✓
Voicemail	✓	✓
Calendar	✓	✓
Notes	✓	✓
Maps Bookmarks	✓	✓
Maps History	✓	✓
Maps Directions	✓	✓
Mac Address	✓	✓
Installed Applications	✓	✓

Data Type	Standard Devices	Jailbroken Devices
Email Messages	✗	✓
Safari Bookmarks	✗	✓
Safari History	✗	✓
Safari Suspend State	✗	✓
YouTube Bookmarks	✗	✓
Dynamic Text	✗	✓
WiFi Locations	✓	✓
Cell Locations	✓	✓
Mail Accounts	✗	✓
Filesystem	✗	✓
Parsed Recovered Data		
SMS Search	✗	✓
Messages	✓	✓
Safari Bookmarks	✓	✓
Notes	✓	✓
Call logs	✓	✓

Data Type	Standard Devices	Jailbroken Devices
Contacts	✓	✓
Contacts Properties	✓	✓
WiFi Locations	✓	✓
Cell Locations	✓	✓
Other Data		
Device Properties	✓	✓

Acquired data is parsed according to the following table:

Data Type	Data Format
Contacts	A grid containing the fields: • Creation Date (GMT) • Department • Display Name • First Name • Last Name • First Fonetic • Job Title • Middle Name • Middle Fonetic • Modification Date (GMT) • Nickname • Note • Organization • Phone Number 1 • Phone Number 2 • Phone Number 3 • Phone Number 4 • Email Address 1 • Email Address 2 • Email Address 3 • Phone Number 1 • Phone Number 2 • Phone Number 3 • Phone Number 4 • Phone Number 5 • Phone Number 6 • Phone Number 7 • Phone Number 8 • Phone Number 9 • Phone Number 10 • Ringtone • Sound for SMS • Web Site 1 • Web Site 2 • Web Site 3 • Web Site 4

Data Type	Data Format
Contacts Properties	A grid containing the fields: • Value • Property Type • Raw Data
Messages	A grid containing the fields: • Type • Name • Number • Text • Subject • Sent(GMT) • Received(GMT) • Read(GMT) • Service • Error • Is Sent • Attachments • iMessage Sent as SMS • User Account **Note:** Service Center Depending on the device type (standard or jailbroken) some fields may not be present.
SMS Search	A grid containing the fields: • Title • Summary • Raw data **Note:** The SMS Search feature is acquired only from devices with iOS 5.x and later.

<table>
<tr><th>Data Type</th><th>Data Format</th></tr>
<tr><td>Call history</td><td>A grid containing the fields:
For iOS 7.x devices:
Number
Date (GMT)
Duration (sec)
Type
For iOS 8.x and later devices:
Number/E-mail
Date (GMT)
Country Code
Type
Duration
Call Method
Missed Call Notification
FaceTime Traffic Size (MB)
Note: For iOS 8.x and higher devices, two grids may be present: Call History 1.x–7.x (call history from before the update to 8.x) and Call History 8.x (call history after the update to 8.x; sometimes it may include the call history from before the update).</td></tr>
<tr><td>iMessages</td><td>A grid containing the fields:
User Account
Type
Text
Date Sent
Date Created/Received
Contact
Date Read
Attachments
Note: The iMessages feature is acquired only from devices with iOS 5.x and later.</td></tr>
</table>

<table>
<tr><th>Data Type</th><th>Data Format</th></tr>
<tr><td>Voicemail</td><td>A grid containing the fields:
Sender
Date
Status
Callback Number
Duration (sec)
Expiration Date
Trashed Date
Path</td></tr>
<tr><td>Calendar</td><td>A grid containing the fields:
Summary
Location
Description
Start date
Start timezone
End date
All day
Calendar ID</td></tr>
<tr><td>Notes</td><td>A grid containing the fields:
Creation date
Title
Summary
Note: For devices with iOS 8.x parsing of notes is not fully supported in the current version of DS.</td></tr>
</table>

Data Type	Data Format
Email messages	Binary nodes for not parsed data and grid for parsed data. A grid containing the fields: • Data • Extended data • Sender • Recipient • Subject • Date sent • Date received • Mailbox • Remote mailbox • Original mailbox • Read • Deleted • MailAccount
Maps Bookmarks	A grid containing the fields: • Name • Locality • Country • Country code • Region • Address book record ID • Address book address ID • Type • Address 1 • Address 2 • Thoroughfare • Latitude • Longitude • Maps URL • Map type • Original type • Zoom level

Data Type	Data Format
Maps History	A grid containing the fields: • Query • Display query • Latitude • Longitude • Latitude span • Longitude span • Location • Has multiple locations • History item type • Zoom level • Start address • Start address type • Start latitude • Start longitude • End address • End address type • End latitude • End longitude • Search kind • Start search result name • Start search result locality • Start search result address 1 • Start search result address 2 • Start search result country • Start search result country code • Start search result region • Start search result postal code • Start search result thoroughfare • Start search result type • Start search result latitude • Start search result longitude • Start search result maps URL • Start search result original type • Start search result zoom level • Start search result map type • End search result name • End search result locality

Data Type	Data Format
	• End search result address 1 • End search result address 2 • End search result country • End search result country code • End search result region • End search result postal code • End search result thoroughfare • End search result type • End search result latitude • End search result longitude • End search result maps URL • End search result original type • End search result map type • End search result zoom level
Maps Directions	A grid containing the fields: • Start search result zoom level • Start search result map type • Start search result name • Start search result latitude • Start search result maps URL • Start search result longitude • Start search result thoroughfare • Start search result type • Start search result original type • End search result zoom level • End search result map type • End search result name • End search result latitude • End search result maps URL • End search result longitude • End search result thoroughfare • End search result type • End search result original type
Safari Suspend State	A grid containing the fields: • Document • Document last visited time (GMT) • Document UUID • Document title

Data Type	Data Format
Safari History	A grid containing the fields: • UUID • Title • URL
Safari Bookmarks	A grid containing the fields: • Last visited data (GMT) • Title • Visit count • Link
Mail Accounts	A grid containing the fields: • Account • Username • Hostname • Should use authentication • Unique ID • Account type • SSL is direct • Draft mailbox name • Account path • Sent messages mailbox name • Trash mailbox name • Account name • SSL enabled • Full username • Email address • SMTP identifier • Class • Type string
YouTube Bookmarks	A grid containing the bookmarked YouTube URL links.
Dynamic Text	A grid containing the dynamic text words.

Data Type	Data Format
WiFi Locations	A grid containing the fields: • Latitude • Longitude • Wifi MAC address • Timestamp (GMT) **Note:** This feature is acquired only from standard devices with iOS 4.x and jailbroken devices with iOS 6.x and 7.x.
Cell Locations	A grid containing the fields: • CI • LAC • Latitude • Longitude • MCC • MNC • Timestamp (GMT) **Note:** This feature is acquired only from standard devices with iOS 4.x and jailbroken devices with iOS 6.x and 7.x.
File System	Binary nodes
Mac Address	A sequence of 12 hexadecimal numbers in the Properties pane.
Device Properties	The following device properties are acquired: • Modem firmware (except iPod devices) • IMEI • ICCID (if SIM card is present in a device) • IMSI (if SIM card is present in a device)

<table>
<tr><th>Data Type</th><th>Data Format</th></tr>
<tr><td>Passwords</td><td>This type of data contains several grids with passwords and password related data.
Each grid may contain the following fields:
Service Name
Account
Password (or Data)
Access Group
Type
Description
Comment
Labels
Tags
Creation Date
Modification Date
Source File
Note: The number of fields may vary for each grid.</td></tr>
</table>

<table>
<tr><th>Data Type</th><th>Data Format</th></tr>
<tr><td>Installed Applications</td><td>This type of data contains the information on the applications installed on the device and parsed application data.

Note: The Installed Applications feature is acquired only from devices with iOS 3.1.3 and higher.

The Installed Applications List grid contains the following data:
Icon (the icon that appears in the list of installed applications in a device)
Application Name (the name of the application as it appears in the list of installed applications on the device)
Internal Application Name (a unique identifier of the application)
Category (the category of applications to which the application belongs as it is shown in App Store)
Manufacturer (the name of the application manufacturer)
Signer Identity (the application signature)
Min OS Ver (minimal iOS version under which the application can operate)
Version (the version of the application)
Data Usage (data used by the application)
Parsed Application Data (if available, contains a link to the parsed application data)
Raw Application Data (contains a link to the unparsed application data in the device file system)
The Application Data folder contains various grids with parsed data of installed applications. In the current version of DS, parsing is performed for the following applications:
DJI Go
Evernote
Facebook Messenger (version 13 and later)
Google Chrome
Google Maps
Gmail
Note: The Recovered Contacts grid may contain invalid data if the corresponding data on the device is corrupted.
Jott Messenger
Kik (Kik Messenger)</td></tr>
</table>

Data Type	Data Format
	Note: The grid Messages Marked as Deleted does not contain recovered data. These messages are marked as deleted, but are not deleted from the device. • LinkedIn • MailRu (Mail.ru) • Skype • Tinder • Twitter • TextFree (Text Free: Free Texting App + Free Calling App + SMS with Textfree) • TextPlus (textPlus Free Text + Calls : Free Texting + Free Phone Calling + Free International Messenger) • VK • WhatsApp (WhatsApp Messenger) • Whisper • Yik Yak **Note:** The amount of acquired application data depends on the volume of data stored in the cache of the corresponding application in the device.

Note: For Parsed Recovered Data, fields in any data type may contain an N/A value if corresponding data was not parsed. This might happen because deleted data associated with an item in the list was partly overwritten by the device OS.

You can view the parsed application data in the Application Data folder.

Physical acquisition of iPhone/iPad/iPod Touch devices allows you to acquire the following groups of data:

- Completely acquired System and User file systems in binary files
- Parsed Data (as in iPhone/iPad/iPod Touch logical acquisition without Installed Applications)
- Deleted data in parsed format (including Address Book, Calendar, Call History, iMessages, Network Connection, Notes, Safari Bookmarks, Messages, and SMS Search) and deleted unparsed data (as in the iPhone/iPad/iPod Touch Advanced (logical) plug-in)

Note: Depending on the iOS version, some features may not be acquired.

- Bit-by-bit image of the device flash memory

  Note: The resulting size of the bit-by-bit image is equal to the size of the device flash memory.

Usually the amount of acquired data depends on the model and state of the device.

Supported Models

Support of physical acquisition is determined based on the hardware. The following models are supported:

iOS Device Hardware	Logical	Physical
iPhone 1G	✓	✕
iPhone 2G	✓	✕
iPhone 3G	✓	✓
iPhone 3GS	✓	✓
iPhone 4G	✓	✓
iPhone 4S	✓	✓ (Jailbroken only)
iPhone 5	✓	✓ (Jailbroken via TaiG only)
iPhone 5C	✓	✓ (Jailbroken via TaiG only)
iPhone 5S	✓	✓ (Jailbroken via TaiG only)
iPhone 6	✓	✓ (Jailbroken via TaiG only)
iPhone 6 Plus	✓	✓ (Jailbroken via TaiG only)
iPhone 6s	✓	✕
iPhone 6s Plus	✓	✕
iPhone SE	✓	✕
iPhone 7	✓	✕
iPhone 7 Plus	✓	✕
iPhone 8	✓	✕

iOS Device Hardware	Logical	Physical
iPhone 8 Plus	✓	✕
iPhone X	✓	✕
iPad 1st Gen	✓	✓
iPad 2nd Gen	✓	✕
iPad 3rd Gen	✓	✕
iPad 4th Gen	✓	✕
iPad 5th Gen	✓	✕
iPad Air	✓	✕
iPad Air 2	✓	✕
iPad Mini 1st Gen	✓	✕
iPad Mini 2nd Gen	✓	✕
iPad Mini 3rd Gen	✓	✕
iPad Mini 4th Gen	✓	✕
iPad Pro	✓	✕
iPod Touch 1st Gen	✓	✕
iPod Touch 2nd Gen	✓	✕
iPod Touch 3rd Gen	✓	✓
iPod Touch 4th Gen	✓	✓
iPod Touch 5th Gen	✓	✕
iPod Touch 6th Gen	✓	✕

The following iOS versions are supported:

iOS Version	Logical Support	Physical Support
1.x	✓	✓
2.x	✓	✓
3.x	✓	✓
4.x	✓	✓
5.x	✓	✓
6.x	✓	✓
7.0.x	✓	✓
7.1	✓	✓
7.1.1	✓	✓
8.0.x	✓	✓
8.1.x	✓	✓
8.2.x	✓	✓
8.3	✓	✓
8.4	✓	✓
9.0	✓	✕
9.1	✓	✕
9.2	✓	✕
9.2.1	✓	✕
9.3	✓	✕
9.3.1	✓	✕
10.0	✓	✕
10.0.1	✓	✕
10.0.2	✓	✕

iOS Version	Logical Support	Physical Support
10.0.3	✓	✕
10.1	✓	✕
10.1.1	✓	✕
10.2.x	✓	✕
10.3.x	✓	✕
11.0.x	✓	✕

iPhone/iPad/iPod Touch FAQ

Q: The iPhone doesn't connect to the computer. What do I do?

A: Please try one of the following:

- If the device you are trying to acquire has been successfully connected to another PC previously, you can try copying the content of the Lockdown folder (by default its location is `C:\Program Data\Apple\Lockdown`) to the same folder on your PC.
- Make sure that no programs, such as a firewall, block EnCase Forensic access to the network.
- The iPhone battery might need to be recharged.
- Disconnect other USB devices from your computer and connect the iPhone to a different USB 2.0 port on your computer.
- Turn the iPhone off and turn it on again. Press and hold the **Sleep/Wake** button on the top of the iPhone for a few seconds until a red slider appears, and then slide the slider. Then press and hold the **Sleep/Wake** button until the Apple logo appears.
- Restart your computer and reconnect the iPhone to your computer.
- Download and install (or reinstall) the latest version of iTunes from www.apple.com/itunes.

Q: I can't acquire data from this device. Why?

A: First try the following:

- Try uninstalling the Apple software components and then reinstall the Mobile Driver Pack. Follow the Apple support instruction (http://support.apple.com/kb/ht1923) to properly uninstall Apple software components. After this, uninstall the Mobile Driver

Pack and install it again.

- For physical acquisition of non-jailbroken devices, check that you have correctly put the device in DFU mode. Follow the instructions in the Data acquisition section. If the device is placed into the DFU mode, there must be no logos on the screen.

See also General Acquisition FAQ for more information.

Q: I have a jailbroken device, but I cannot acquire application data. How can I fix this?

A: You need to install the House Arrest tweak (http://cydia.saurik.com/package/com.npupyshev.mobile.house-arrest/) to be able to acquire application data. Please note that this tweak also requires the Cydia application to be installed on the device.

Q: The device is locked with a password. Is there a way to acquire it?

A: Yes. If the device you are trying to acquire has been successfully connected to another PC previously, you can try copying the content of the Lockdown folder (by default its location is `C:\Program Data\Apple\Lockdown`) to the same folder on your PC. Please note that this will only work if the password on the device was set before the device was connected to the PC.

Q: The acquisition process was broken. The device is in the Recovery mode. What do I do?

A: Start acquisition of the device once more. If you don't want to acquire data, just wait until the device restarts and disconnect it from the computer.

Q: The iPhone hung. What do I do?

A: Reset the iPhone by holding the **Sleep/Wake** button at the top right of the device and the Home button at the bottom center of the face at the same time.

Q: What's the difference between the iPhone/iPad/iPod Touch Advanced Logical and the iPhone/iPad/iPod Touch Physical plug-ins?

A: The iPhone/iPad/iPod Touch Physical plug-in allows you to acquire all data from your iPhone/iPad/iPod Touch device. The amount of parsed data both in logical and physical plug-ins is the same. But the total amount of data is larger in the physical plug-in. It contains the file system that is inaccessible for the logical plug-in.

Q: The acquisition from my iPhone/iPad/iPod Touch device interrupts. Why?

A: iPhone/iPad/iPod Touch devices with iOS 7 and later require you to establish trusted connection after connecting it to the computer and on the start of acquisition. For this purpose, you need to tap Trust on the device each time a message appears on the device screen.

Q: I get the message that limited application data has been acquired. What does it mean?

A: Generally, it means that the version of the application on your device is higher than the one supported in the current version of EnCase Forensic . Please contact technical support.

Q: My jailbroken iOS device is acquired as a not jailbroken device. Why?

A: You need to install a special AFC2 tweak to unlock the device file system. To install the tweak:

1. Open Cydia on the device.
2. On the Cydia home screen, tap **Sources** > **Edit** > **Add**.
3. Enter `apt.taig.com` in the text box and then tap **Add Source**.
4. The TaiG source adding starts.
5. After the source is added, tap TaiG in the Sources list and select **All Packages**.
6. Tap TaiG AFC2 in the list.
7. Tap Install and then tap **Confirm** to install the tweak.
8. Reboot the device.
9. The tweak is now installed.

DATA ACQUISITION - IPOD

Only physical acquisition can be performed on an iPod. Physical acquisition is performed via the **iPod Physical Plug-in**.

Data acquisition is performed using the standard process.

ACQUIRED DATA - IPOD

All data is parsed, from the FAT filesystem to binary files. In addition, the following data is detected and located in separate folders as binary files:

- Device
- Accessories
- iTunes
- Music

- Contacts (contacts are stored in the vcard format)
- Calendars (calendars are stored in the vcalendar format)
- Notes

IPOD FAQ

Q: The iPod doesn't connect to the computer. What do I do?

A: Please try one of the following:

- Make sure that no programs or firewalls block EnCase Forensic access to the network .
- If that doesn't work, disconnect other USB devices from your computer and connect the iPod to a different USB 2.0 port on your computer.
- If that doesn't work, turn the iPod off and turn it on again.
- If that doesn't work, restart your computer and reconnect the iPod to your computer.
- If that doesn't work, download and install (or reinstall) the latest version of iTunes from www.apple.com/itunes.

See also General Acquisition FAQ for more information.

Acquiring Data from Android OS Devices (Including Kindle Fire Tablets and Android Wear)

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

About Data Acquisition from Android OS Devices

The program allows you to acquire information from devices running Android OS 7.1 and lower. This includes such devices as smart phones, Android wear devices, and Kindle Fire tablets.

Depending on the manufacturer and the model of your device and the data you want to acquire, different plug-ins must be used:

Device Type	Rootable during Acquisition	Autodetect	Plug-In
LG devices with Android OS 4.4.2–5.1.1	×	×	Android LG Advanced Physical
Samsung devices with Android OS 4.4.4–7.1	×	×	Android Samsung Bootloader Physical
Other devices with Android OS 4.4.4 and lower	✓	✓	Android Logical Android Physical
Other devices with Android OS 5.0–7.1	×	✓	Android Logical

Note: Any device with Android OS 7.1 and lower can be acquired via the Android Logical plug-in regardless of its manufacturer and model. If the device is locked, you can try to acquire it using the Android Samsung Bootloader Physical or Android LG Advanced Physical plug-in if the plugin support the corresponding device model.

Android Device Rooting

Rooting is a process of acquiring root-level access to the device file system, which allows you to do the following:

- Recover and acquire deleted data on the device.
- Acquire data from applications installed on the device.
- Extract device authentication data.
- Acquire the full file system of the device.
- Remove device password protection.
- Perform full physical acquisition of the device memory.

Rooting can be performed either by the user prior to acquisition, or by the program during an acquisition. In the latter case, rooting is temporary and all effects of device rooting are reverted after acquisition finishes.

In the program, rooting can be performed for the majority of devices with Android OS 4.4.4 and lower. Rooting of devices with higher Android OS is not possible in most cases. Please also note that some device models or model lines with Android OS 4.4.4 and lower may have custom modifications, which makes it impossible to root them.

Android OS Devices

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Installing Android Drivers from Device

Drivers for most Android devices are included in the Driver Pack, but for some newest devices, drivers must be installed from the device itself.

To install drivers from a device:

1. Turn the device on and connect it to your computer.
2. On the device, swipe down from the top of the screen.
3. Tap the USB connection selection menu (it will have the Touch for other USB options message).
4. Select **Install driver** in the menu.
5. On your computer, go to **My Computer** and double click the drive named **USB_Driver**.
6. Double click the AutoRun.exe file.
7. The USB Driver Setup wizard opens.
8. Follow the instructions in the setup wizard to install the required drivers.
9. After the installation finishes, click **Finish** in the wizard.
10. On the device, swipe down from the top of the screen again.
11. Tap the USB connection selection menu.
12. Select **Mass Storage** in the menu.
13. The drivers are installed, and the device is now ready for acquisition.

Preparing Device for Acquisition

The program allows you to acquire Android OS phones, Android Wear devices, and Kindle Fire tablets using the same plug-ins. Please note that these devices require different actions to be performed to prepare them for acquisition.

To prepare an Android OS phone/Android Wear device for the acquisition:

1. Enable installation from unknown sources on the device:
    - **For Android OS lower than 4.0:** Select **Settings > Application Settings** and select the **Unknown sources** option.

        Note: For Android OS 1.5, there is no such option and enabling it is not required.

    - **For Android OS 4.0 and higher:** Select **Settings > Security** and select the **Unknown sources** option.

2. Enable the USB debugging mode on the device:
    - **For Android OS up to version 3.0:** In the device menu, select **Settings > Applications > Development** and select the **USB debugging** option.
    - **For Android OS from 4.0 and up to 4.1:** In the device menu, select **Settings > Developer** options and select USB debugging.
    - **For Android OS 4.2 and newer:** In the device menu, select **Settings > About** device/tablet and tap **Build number** seven times, then go back to **Settings**, select **Developer options**, and then select **USB debugging**.

3. Tap **OK** in the confirmation message.
4. Connect the device to the computer using a data cable. Make sure the required drivers are installed (the required drivers for most Android devices are included in the Mobile Driver Pack).

To prepare a Kindle Fire device for acquisition:

1. Enable the ADB on the device:
    - For the 2nd generation devices: Select **Settings > Security > Enable ADB**.
    - For the 3rd generation devices: Select **Settings > Device > Developer Options > Enable ADB**.
    - For the 4th generation devices: Select **Settings > Device > Developer Options > Enable ADB**.

        Note: For the 1st generation Kindle Fire devices, the required option is enabled by default.

2. Tap **Enable** in the confirmation message.
3. Connect the device to the computer using a data cable. Make sure the required drivers are installed (the required drivers for most devices are included in the Mobile Driver Pack).

Data Acquisition - Android

The processes of logical and physical acquisition of Android OS devices are performed following the same steps.

> **Note:** WARNING! During data acquisition, your device may reboot a few times and you will need to enter its PIN/password. Make sure you know the device PIN before performing acquisition. For devices with Android OS up to 4.1, if the phone is in the USB debugging mode, the program can bypass the PIN/password.

Logical acquisition is performed via the **Android Logical Plug-in**.

Physical acquisition is performed via the **Android Physical Plug-in**.

To acquire the device:

1. Prepare the device for acquisition.
2. Follow the standard process of acquisition.
3. Before starting acquisition, on the Pre-acquisition Options page, do the following:
   - Select **Unlock device file system** to unlock the device file system. This action is required to perform acquisition.

     > **Note:** Unlocking a device file system doesn't damage the device or any data on it.

   - Select **Remove password protection** to remove any screen password protection on the device (password, graphical password, and PIN). This feature is available only for Android OS up to version 4.1.

     > **Note:** If the screen password still appears after removal, simply draw any pattern to remove a graphical password or enter and confirm a new PIN or password.

4. Move between the other pages of the wizard and, when you are ready to start acquisition, click **Start Acquisition**.
5. Before acquisition starts, the device file system will be unlocked. The file system unlocking process is performed as follows: the **AndroidService.apk** installation package is written to the `/data/local/tmp` folder and a special service is installed to the system folder with applications. They will be removed automatically after the acquisition process finishes.

   > **Note:** This does not damage data integrity and doesn't cause any damage to the device.

6. Data acquisition starts, and its process is displayed on the Acquisition Progress page.

7. During acquisition, the following messages may appear on the device:
    - If the **Allow USB Debugging** message appears on the device, tap **OK** in it to continue acquisition.
    - If the **Full Backup** message appears on the device, tap Back up my data in it to continue acquisition. This message appears if device rooting failed. In this case, backing up data on the device allows acquiring at least some part of the device file system.
    - If the **Waiting For Debugger** message appears on the device, do not close the message or the acquisition process will fail. This does not affect data integrity on the device.
    - If the **Choose Connection Mode** message reappears on the device, choose the connection mode.

8. When data acquisition finishes, the case is saved. Click **Finish**.

    Note: This process may take some time.

9. Disconnect your device from the computer.

Acquired Data - Android

Logical acquisition acquires the following groups of data:

Data Type	Not Rooted Devices	Rooted Devices
Parsed Actual Data		
Contacts	✓	✓
SMS History	✓	✓
MMS History	✓	✓
File system (including SD card content)	Partially	✓
Call History	✓	✓
Media Store	✓	✓
Browser History	✓	✓
Settings	✓	✓

Data Type	Not Rooted Devices	Rooted Devices
Calendar	✓	✓
Installed Applications	✓	✓
Application Data	✗	✓
Authentication Data	✗	✓
Parsed Recovered Data		
Contacts	✗	✓
SMS History	✗	✓
MMS History	✗	✓
Call History	✗	✓
Calendar	✗	✓
Multimedia and graphic files (from SD card)	✗	✓
Other Data		
Device Properties	✓	✓

Acquired data is parsed according to the following table:

Data Type	Notes	Data Format
Contacts	Numbers stored in the Phone memory and the folder with photos (including deleted data)	A grid containing the fields: • Photo • Name • Notes • Phone (home) • Phone (mobile) • Email (home) • Email (work) • Email (other) • IM • Postal • Organization • Times contacted
SMS History	Both sent and received SMS and a folder with the attachments shown in the binary files (including deleted data)	The SMS History is a grid containing the fields: • Date • Read • Address • Status • Type **Note:** For Parsed Recovered SMS History, the Type column contains the following values: 1 – Inbox 2 – Sent 3 – Draft 4 – Outbox 5 – Failed • Subject • Body • Service Center

Data Type	Notes	Data Format
MMS History	Both sent and received MMS, and a folder with the attachments shown in the binary files (including deleted data)	The MMS History is a grid containing the fields: • Date • Read • Address • Priority • Box • Class • Type • Subject • Text • Image • Image 1 • Image 2 • Delivery report • Expiry • MMS version • Read report • Audio
Call History	History of call logs (dialed numbers, received calls, etc)	A grid containing the fields: • Date • Type • Duration • New • Number • Number type • Name

Data Type	Notes	Data Format
Media Store	Information from the Image, Audio, and Video stores	Video store is a grid containing the fields: • Name • Title • Size • MIME type • Date added • Date modified • Date taken • Duration • Resolution • Artist • Album • Category • Description • Private • Data Image store is a grid containing the fields: • Name • Title • Size • MIME type • Date added • Date modified • Date taken • Description • Private • Data • Orientation Audio store is a grid containing the fields: • Name • Title • Size • MIME type • Date added

Data Type	Notes	Data Format
		• Date modified • Duration • Artist • Composer • Album • Track • Year • Alarm • Music • Notification • Ringtone • Data
Browser History	Includes browser history including visited URLs and performed searches.	URL history is a grid containing the fields: • Title • URL • Date • Bookmark • Visits Search history is a grid containing the fields: • Text • Date
Settings	System settings of the device	A grid containing the fields: • Name • Value
Calendar	Events and Calendar data stored on the phone.	The grids containing fields corresponding to the displayed data.

<table>
<tr><th>Data Type</th><th>Notes</th><th>Data Format</th></tr>
<tr><td>File system</td><td>The amount of data acquired depends on the model of the phone and its state.</td><td>Binary nodes

Content of an SD card inserted in a device (the \File System\mnt\sdcard folder).

Please note that while acquiring device file system with the logical plug-in, the files and folders locked by the device OS will not be acquired (they are displayed with a lock icon in the Case pane). These files and folders include:

• /proc/
• /dev/
• /sys/devices/
• /sys/class/power_supply/ac/
• /sys/kernel/slab/
• /sys/kernel/debug/
• /sys/module/
• /sys/android_power/wait_for_fb_sleep
• /sys/android_power/wait_for_fb_wake
• /sys/power/wait_for_fb_sleep
• /sys/power/wait_for_fb_wake
• /sys/module/mddi/parameters/emdh_val
• /sys/module/mddi/parameters/pmdh_val
• /dev/graphics/
• /dev/input/
• /dev/log/
• /dev/urandom
• /dev/random
• /dev/full
• /dev/zero
• /dev/ptmx
• /clock_source</td></tr>
</table>

Data Type	Notes	Data Format
Android Backup	Includes only backup file from which file system data is parsed in case device rooting failed.	Android Backup.ab binary file.

Data Type	Notes	Data Format
Installed Applications	The amount of acquired application data depends on the volume of data stored in the cache of the corresponding application in the device.	This type of data contains the information on the applications installed on the device and parsed application data. The Installed Applications List grid contains the following data: • Icon (the icon that appears in the list of installed applications in a device) • Application Name (the name of the application as it appears in the list of installed applications on the device) • Version (the version of installed application) • Internal Application Name (a unique identifier of the application) • Category (the category of applications to which the application belongs as it is shown in Play Store) • Manufacturer (the name of the application manufacturer) • Parsed Application Data (if available, contains a link to the parsed application data) • Raw Application Data (contains a link to the unparsed application data in the device file system) • Application Permissions (contains a link that opens the list of application permissions in the device system) The Application Data folder contains various grids with parsed data of installed applications. In the current version of EnCase Endpoint Investigator, parsing is performed for the following applications: • Facebook • Facebook Messenger

Data Type	Notes	Data Format
		• Fitbit • Google Chrome • Instagram • Jott Messenger • Kik (Kik Messenger) • LinkedIn • Pinger (Free Texting App Text Free) • Skype • Snapchat • textPlus • Textfree (Text Free: Free Texting App) • Tinder • Vkontakte • WhatsApp (WhatsApp Messenger) • Whisper If an application was moved to an external memory card, it won't be parsed.

All data is acquired using the USB, Android Debug Bridge, and the program internal protocols.

> **Note:** Acquisition of the device filesystem and recovery of deleted data are not guaranteed for devices with Android OS 2.3.6.

The device properties are acquired and displayed in the Properties pane.

Physical acquisition acquires the following groups of data:

- **Full Flash:** Full flash includes raw partition images and parsed deleted data.
- **File system:** File system content is displayed in binary nodes.

The device properties are acquired and displayed in the Properties pane.

Supported Models - Android

The program supports acquisition from rooted or rootable Android OS phones, Android Wear devices, and Kindle Fire tablets with Android OS 7.1 and earlier for logical acquisition and Android OS 4.4.4 and earlier for physical acquisition.

> **Note:** Physical acquisition of devices based on Android OS 2.3.6 is not guaranteed.

Android devices vary by manufacturer. Each manufacturer has the ability to modify the device and it can affect the support of the device within the program. Guidance Software tests on a variety of devices from a variety of manufacturers, but that does not guarantee 100% support of all Android devices running a particular firmware because of these manufacturer changes. If your device firmware is supported, but your device is not processed, please gather the logs and send them to our support team. This will allow us to add modifications in future releases to account for the manufacturer differences on the device you were processing.

Android OS Devices FAQ

Q: I can't acquire data from this device. Why?

A: Try installing drivers from the device manufacturer website.

See also General Acquisition FAQ for more information.

Q: The acquisition fails on my Motorola MB200 device. Why?

A: On the start of acquisition of Motorola MB200 device, the device automatically reconnects to the PC and the Choose Connection Mode message reappears on the device. Choose the connection mode.

Q: I get the message that limited application data has been acquired. What does it mean?

A: Generally, it means that the version of the application on your device is higher than the one supported in the current version of EnCase Mobile Investogator. Please contact Technical Support.

Q: I cannot acquire an Android backup file. Why?

A: An Android backup file is acquired only in case device rooting failed. If device rooting is successful, the acquired data contains all files that may be included in a backup file; therefore, the acquisition of an Android backup file is not necessary.

LG Devices with Android OS 4.4.2 - 5.1.1

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process.

This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Preparing Device for Acquisition - LG

EnCase Forensic allows you to acquire advanced Android LG smartphones and Android LG smartwatches.

To be able to perform acquisition of an advanced Android LG smartphone, do the following to prepare the device for acquisition:

1. Turn off the device.
2. Press and hold the **Volume Up** button.
3. Connect the device to a computer using a USB cable while still holding the button.
4. Keep the **Volume Up** button pressed until the device enters Download Mode.
5. Wait until the required drivers are installed.
6. The device is now in Firmware Update mode.

> **Note:** To return the device to a normal mode, simply press and hold the Power button or remove the battery and place it back.

To be able to perform acquisition of an advanced Android LG smartwatch, do the following to prepare the device for acquisition:

1. Turn off the device.
2. Connect the device to a computer.
3. Swipe the device screen from the bottom-left to the top-right corner to put the device into Download Mode.
4. The device is in the Firmware Update mode now.

> **Note:** To return the device to a normal mode, simply disconnect it.

Data Acquisition - LG

The program allows you to perform physical acquisition of advanced Android LG devices using the Android LG Advanced Physical plug-in.

Data acquisition is performed using the standard process.

> **Note:** In the current version of the program, acquisition of advanced Android LG devices can be performed only via manual plug-in selection.

Acquired Data - LG

The Android LG Advanced Physical plug-in acquires a complete file system of a device. The file system is parsed and its content is shown in the form of binary files.

Supported Models - LG

The Android LG Advanced Physical plug-in allows you to acquire the following models of Android LG devices with Android OS 4.4.2–5.1.1:

- LG G4
- LG G3 (all variants)
- LG G3 Beat
- LG G2 (all variants)
- LG G2 Mini
- LG G Pro 2
- LG G Pad
- LG G Watch
- LG F60
- LG L90
- LG Tribute
- LG Spirit
- LG Volt
- LG G Vista

Advanced Android LG Devices FAQ

Q: The device does not enter the Firmware Update mode and enters the battery charging mode instead. Why?

A: The device may have been connected to a computer before pressing the **Volume Up** button, or the button was released too early.

Q: Can I acquire other devices with Android 4.4.2 – 5.1.1 using the Android LG Advanced Physical plug-in?

A: The Android LG Advanced Physical plug-in works only for LG devices and only with a limited number of models. Successful acquisition of other LG models is not guaranteed.

Q: I cannot acquire data from my smartwatch device. How can I fix this?

A: If you have problems acquiring smartwatches, try one of the following solutions:

- Disconnect the device from a computer and connect it back again.
- In the Windows Device Manager, find your smartwatch device, click **Update Driver Software** in the device context menu, and select **Search automatically for updated driver software**.

Samsung Devices with Android OS 4.4.4 – 6.0.1

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Preparing Device for Acquisition - Samsung

The program allows you to acquire Samsung devices running Android OS 4.4.4 – 6.0.1.

To prepare a Samsung smartphone with Android OS 4.4.4 – 6.0.1 for acquisition, put it into the Download mode:

1. Turn off the device.
2. Press and hold the **Volume Down**, **Home**, and **Power** buttons, all at the same time.
3. Release the buttons only when the **Warning** message appears.
4. Press the **Volume Up** button.
5. When your device shows a green Android icon with the **Downloading... Do not turn off target** text under it, connect it to your PC.

Data Acquisition - Samsung

The program allows you to acquire Samsung smartphones running Android 4.4.4 – 6.0.1 using the Android Samsung Bootloader Physical plug-in.

> **Note:** In the current version of the program, acquisition of Android Samsung devices can be performed only via manual plug-in selection.

To perform acquisition, a custom forensic recovery image file has to be written into your device memory. Once it is done, you will need to reboot your device into Recovery mode.

> **Note:** Please keep in mind that the firmware of your device will be changed as a result of acquisition by this plug-in.

To acquire the device via manual plug-in selection:

1. Prepare the device for acquisition.
2. Follow the standard process of acquisition.
3. On the **Model Selection** page of the wizard, select the model of your device and click **Continue**.
4. On the **Connection Selection** page, select the connection type and click **Start Acquisition**.
5. The **Acquisition page** opens.
6. Wait while a forensic recovery image file is being written into your device memory. The progress is displayed in the Flashing status line.
7. Once the program has written the forensic recovery image file into your device memory, a dialog window opens with an instruction on how to reboot your device in the Recovery mode. Follow the instructions and reboot your device.
8. After your device is rebooted into Recovery mode, the acquisition starts automatically. The progress of acquiring the flash partitions and the file system of your device is displayed in the Flash Partitions and File System status lines, respectively.
9. After the acquisition finishes, click **Finish**.
10. The case is saved. Disconnect the device from the computer.

Acquired Data - Samsung

The Android Samsung Bootloader Physical plug-in allows you to acquire the full file system and flash memory of an Android Samsung device.

Supported Models - Samsung

The Android Samsung Bootloader Physical plug-in allows you to acquire the following Samsung devices:

- Samsung Galaxy S5 (SM-G900P)
- Samsung Galaxy S6 (SM-G920I)
- Samsung Galaxy S6 (SM-G920F)
- Samsung Galaxy S6 (SM-G920K)
- Samsung Galaxy S6 (SM-G920L)
- Samsung Galaxy S6 (SM-G920P)
- Samsung Galaxy S6 (SM-G920S)

Note: If your device model is not on this list, please do not try to acquire it via the Android Samsung Bootloader (Physical) plug-in. This may result in your device not being functional after your acquisition is complete.

Samsung Devices with Android 4.4.4 - 6.0.1 FAQ

Q: Can I try to acquire a device if it is not on the list of supported devices?

A: No. If the device model you are trying to acquire does not correspond to the model you select in the Acquisition Wizard, the device data may be wiped completely.

Q: The device starts normally when I try to put it into the Download Mode. Why?

A: This may happen if the **Volume Down**, **Home**, and **Power** buttons are released too early, or if they are not pressed simultaneously. Do not release the buttons until the device enters Download Mode.

Android Spreadtrum Devices

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Preparing Environment for Acquisition - Spreadtrum

To prepare the environment for acquisition of Android devices based on Spreadtrum chipsets:

1. Install the Firmware Update drivers for the device.
2. Download the ROM image file to your computer.

Data Acquisition - Spreadtrum

The program allows you to acquire Android devices based on Spreadtrum chipsets using the Android Spreadtrum Expert Physical plug-in.

> **Note:** In the current version of the program, acquisition of devices based on Spreadtrum chipsets can be performed only via manual plug-in selection.

To acquire the device via manual plug-in selection:

1. Prepare the environment for acquisition.
2. Turn off the device and disconnect it from the computer.
3. Follow the standard process of acquisition.
4. On the **Pre-acquisition Options** page, click **Browse** next to the Image file path field and navigate to the downloaded ROM image file.
5. While the device is turned off, press and hold the **Volume Up** button on it.
6. Connect the device to the computer without releasing the **Volume Up** button.

7. Click **Continue** on the Pre-acquisition Options page.

 Note: You will have only 3–5 seconds to click **Continue** after connecting the device to the computer, after which the device will return to the standard mode. If the time runs out, disconnect the device, remove the device battery, place it back again, and repeat the steps 7–9 again.

8. On the **Connection Selection** page, select the connection type and click **Start Acquisition**.

 Note: The device battery doesn't charge during the acquisition. Depending on the time required to acquire all data from the device, you might need to replace the device battery with an alternative power source, like a DC–DC converter, to prevent the device from shutting down during the acquisition.

9. The acquisition process starts. Its progress is displayed on the **Acquisition Progress** page.
10. After the acquisition finishes, click **Finish**.
11. The case is saved and you can disconnect the device from the computer.

Acquired Data - Spreadtrum

The Android Spreadtrum Expert Physical plug-in acquires data stored in the user space of Android devices based on Spreadtrum chipsets.

Supported Models - Spreadtrum

The Android Spreadtrum Expert Physical plug-in allows you to acquire Android devices based of Spreadtrum chipsets regardless of the Android OS version.

Note: Each device model requires specific Firmware Update drivers and ROM image file to be acquired.

Acquiring Data from Tizen Devices

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Preparing Device for Acquisition- Tizen

To be able to perform acquisition of a Tizen device, do the following to prepare the device for acquisition:

1. In the device menu, select **Settings > Device Info**, and then select the USB debugging option.
2. Connect the device to the computer using a data cable. Make sure the required drivers are installed (the required drivers for most Tizen devices are included in the Mobile Driver Pack).

Data Acquisition- Tizen

Acquisition is performed via the Tizen Logical Plug-in.

To acquire the device:

1. Prepare the device for acquisition.
2. Follow the standard process of acquisition.
3. Before starting acquisition, on the Pre-acquisition Options page, select **Unlock device filesystem** to unlock the device file system. This action is required to perform acquisition.

    Note: Unlocking a device file system doesn't damage the device or any data on it.

4. Move between the other pages of the wizard and, when you are ready to start the acquisition, click Start Acquisition.
5. Before acquisition starts, the device file system will be unlocked. For this purpose, the program writes special files to the `/tmp/`, `/opt/usr/apps/tmp/` and `/home/developer/sdk_tools/gdbserver/ folders`. The files will be removed automatically after the process of acquisition finishes.

    Note: This does not damage data integrity and does not cause any damage to the device.

6. Data acquisition starts, and its process is displayed on the Acquisition Progress page.
7. When data acquisition finishes, the case is saved. Click **Finish**.

    Note: This process may take some time.

8. Disconnect your device from the computer.

Acquired Data- Tizen

The program allows you to acquire the full file system of a Tizen device.

Supported Models - Tizen

The program supports acquisition from devices with Tizen OS 2.2.x – 2.4.

Tizen Devices FAQ

Q: The device doesn't connect to the computer. What do I do?

A: Please try one of the following:

- Make sure that no programs block EnCase Forensic access to the network (e.g., EnCase Forensic is not blocked by a Firewall).
- If that doesn't work, disconnect other USB devices from your computer and connect the device to a different USB 2.0 port on your computer.
- If that doesn't work, turn the device off and turn it on again.
- If that doesn't work, restart your computer and reconnect the device to your computer.
- Make sure you enabled the USB Debugging mode on the device.

See also General Acquisition FAQ for more information.

Acquiring Data from RIM BlackBerry Devices

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Data Acquisition - BlackBerry

Data acquisition of RIM BlackBerry devices is performed using the standard process.

Acquisition is performed via the RIM BlackBerry Plug-in.

> **Note:** If you have BlackBerry Desktop Software installed on your computer, it is necessary to start the software and wait until it connects to the device, otherwise acquisition will fail.

If your device is locked by a password you will be asked to enter it. The password can only be entered 10 times. If you enter a wrong password on the last attempt, all data on the device will be erased.

If acquisition is performed via a COM port and the device is locked by a password, then only the Memory Image can be acquired.

Acquired Data - BlackBerry

The program allows you to acquire the following data from devices:

Please note the following:

- If a BlackBerry device is locked with a password and acquisition is performed via a COM port, databases will not be acquired.
- Memory images from BlackBerry Devices with Java (OS v. 4.0) will probably not be acquired. Their acquisition depends on the state of the device.
- SMS messages once opened on BlackBerry and marked as Unread manually have a Read flag in the program.

The following databases will be parsed:

- Address Book
- Application (OS 4.x and higher)
- Auto Text
- BlackBerry Messenger (OS 4.x and higher)
- Browser Bookmarks
- Calendar
- Categories
- Filesystem (form Content Store database)
- Handheld Agent
- Hotlist
- Memo
- Messages
- PhoneCall
- Profiles
- QuickContacts
- Service Book
- SMS
- Task

Type	Contents
BlackBerry Pager (devices of series 85x)	Memory (in one binary node called Memory Image)
Simple BlackBerry Devices (this devices have Intel 386 processor inside)	Databases stored in the physical memory Some databases are parsed (see list below)
BlackBerry Devices with Java (Devices with OS version 3.7,3.8,4.0)	Memory (in one binary node called Memory Image) Databases stored in the logical memory Content Store contains the following nodes with the binary nodes data format: • samples • home • appdata • system • dev • applications

Supported Models - BlackBerry

Although all models available on the market today cannot be tested, most RIM Blackberry models should work with the program.

There are three groups of supported RIM BlackBerry devices:

- BlackBerry Pagers (series 85x).
- Simple BlackBerry Devices (these devices have the Intel 386 processor).
- BlackBerry Devices with Java (devices with OS version up to 7.1).

RIM BlackBerry FAQ

Q: I cannot acquire Databases and Content Store from this device. Why?

A: Disable the Content Protection option. To do this, set the **Options > Security Options > General Settings > Content Protection** option to **Disabled**, then save your changes and restart the device.

Q: I get the message that limited application data has been imported during the BlackBerry backup 10 import. What does it mean?

A: Generally, it means that the version of the application on your device is higher than the one supported in the current version of EnCase Forensic . Please contact Technical Support.

Acquiring Data from Symbian OS Smartphones

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

About Data Acquisition from Symbian OS Smartphones

The program allows you to acquire information from different types of smartphones running the Symbian OS.

The following types of devices can be acquired:

- Symbian OS 6.0 Devices
- Symbian OS 6.1 Devices
- Nokia Symbian 7.x-8.x
- Nokia Symbian 9.x

Data Acquisition - Symbian 6.0

Data acquisitions are performed using the standard process. This process may take a long time.

> **Note:** Data on the device will not change in the process of acquisition. No data and no applications are written to the device file system.

Acquisition is performed via the Symbian OS 6.0 Devices Logical Plug-in.

> **Note:** Physical acquisition of Nokia Symbian OS devices can only be performed via manual plug-in selection with the Nokia Symbian OS (physical) plug-in.

Acquired Data - Symbian 6.0

The program allows you to acquire the file system from Symbian 6.0 devices.

Disks	Contents	Presence
C:	RAM	It will be empty if a hard reset was done on the device
Z:	ROM	It will always be present
(any letter)	External Disks (D: as a rule)	It can be absent if there are no external disks on the device

Supported Models - Symbian 6.0

Although all models available on the market today cannot be tested, any Symbian OS 6.0 device with a data connection should work with the program.

The following model has been tested:

- Nokia 9290

Data Acquisition - Symbian 6.1

Data acquisition is performed using the standard process.

> **Note:** Data on the device will not change in the acquisition process. No data and no applications are written to the device filesystem.

Acquisition is performed via the Symbian OS 6.1 Devices Logical Plug-in.

Note: Physical acquisition of Nokia Symbian OS devices can only be performed via manual plug-in selection with the Nokia Symbian OS (physical) plug-in.

Please note that Symbian OS 6.1 devices can be connected via IrDA or Bluetooth. We recommend that these forms of connection only be used as a last resort as neither connection is secure. Data cables should always be your first choice as they are secure. Pay attention to the steps for connecting your device using IrDA or Bluetooth.

Note: Symbian OS 6.1 device can be acquired only via manual plug-in selection.

Acquired Data - Symbian 6.1

The Symbian OS 6.1 (logical) plug-in allows you to acquire the files stored in the memory of the device using the PPP protocol.

The following data is acquired:

- Contacts (parsed as a grid)
- Logs, including deleted Logs (parsed as a grid)
- ToDo List (parsed as a grid)
- Calendar (parsed as a grid)
- MailBox (parsed as a grid)
- FileSystem (acquired in binary files, some databases are parsed and placed into the Parsed folder)

Note: The number and names of the fields in the grids depend on device model and settings.

Supported Models- Symbian 6.1

Although all models available on the market today cannot be tested, any Symbian OS 6.1 device with a data connection should work with the program.

Symbian OS 6.1 Devices FAQ

Q: Data is acquired but not parsed. Why?

A: Parsing the acquired data is not yet supported by EnCase Forensic . You can use the hex viewer or other forensic tools to view the data.

Q: I can't acquire data from this device. Why?

A: Check that the IrDA (Bluetooth) connection is correctly set.

See also General Acquisition FAQ for more information.

Data Acquisition - Symbian 7.x - 8.x

Data acquisition is performed using the standard process. This process may take a long time.

Acquisition is performed via the Nokia Symbian 7.x - 8.x Logical Plug-in.

> **Note:** Physical acquisition of Nokia Symbian OS devices can only be performed via manual plug-in selection with the Nokia Symbian OS (physical) plug-in.

Acquired Data - Symbian 7.x - 8.x

The program allows you to acquire the files stored in the memory of the device using the OBEX protocol.

Data Type	Data Format
Contacts	This type of data contains grids with the information on contacts from the acquired device, the last changes made to the contacts list, and configuration for contacts list. Each grid contains the following data: Contacts grid: • ID • Group • Last name • First name • Tel. (home) • Tel. (home) • Web addr. (home) • Street (home) • Postal/ZIP (home) • City (home) • Job title • Job title • Company • Tel. (business) • Mobile (business) • Web addr. (bus.) • P.O. Box (bus.) • Extension (bus.) • Street (business) • Postal/ZIP (bus.) • City (business) • St.Prov. (bus.) • Ctry./Reg. (bus.) • Telephone • Telephone • Mobile • Pager • Fax • Email • Email • Street • City • State/Province

<table>
<tr><th>Data Type</th><th>Data Format</th></tr>
<tr><td></td><td>DTMF
Birthday
Note
User ID
Creation date (UTC)
Last modified (UTC)
Last changes grid:
#
ID
Group
Last name
First name
Job title
Company
Telephone
Mobile
Fax
Email
User ID
Creation date (UTC)
Last modified (UTC)
Config grid:
Parameter
Value</td></tr>
</table>

Data Type	Data Format
Logs	This type of data contains grids with the information on outgoing and incoming calls and messages (including deleted logs) and the grid with configuration for log files. Each grid contains the following data: Logs and Deleted logs grids: • ID • Event type • Direction • Contact ID • Number • Remote party • Subject • Date • Duration • Specific data Config grid: • Parameter • Value

Data Type	Data Format
ToDo list	This type of data contains grids with the information on To Do list acquired from the device and the last changes made to the list. Each grid contains the following data: ToDo list grid: • Description • Priority • Due date • Crossed out date • Creation date Last changes grid: • # • Description • Priority • Due date • Crossed out date • Creation date

<table>
<tr><th>Data Type</th><th>Data Format</th></tr>
<tr><td>Calendar</td><td>This type of data contains grids with the information on the list of calendar events acquired from the device and the last changes made to the list. Each grid contains the following data:

Calendar grid:
#
Status
Description
Location
Type
Start date
Start time
End date
End time
Alarm time
Alarm days warning
Repeat type
Repeat specification
Repeat interval
Repeat forever
Repeat start date
Repeat end date
Creation date
Last changes grid:
#
Status
Description
Location
Type
Start date
Start time
End date
End time
Alarm time
Alarm days warning
Repeat type
Repeat specification</td></tr>
</table>

Data Type	Data Format
	• Repeat interval • Repeat forever • Repeat start date • Repeat end date • Creation date
Mail box	This type of data contains grids with the information on Service Local MTM, SMS, MMS, Wap Push, Email SMTP, Email POP3, and deleted messages acquired from the device. Each grid contains the following data: Deleted messages grid: • Text • Number • Folder • Service • Date Stream SMS Header and Stream Schedule Data grids: • Property • Value
File System	This type of data contains binary nodes grouped by partition labels. Depending on the label, a partition contains the following data: • C: Internal phone memory • D:, E:. etc.: External memory cards (usually store music and multimedia files)
Parsed Databases	This type of data contains databases acquired from the device in binary nodes and grids with various data.

Supported Models - Symbian 7.x - 8.x

Although all models available on the market today cannot be tested, any Nokia device that runs Symbian OS 7.x–8.x should work with the program.

Data Acquisition - Symbian 9.x

Data acquisitions are performed using the standard process.

Acquisition is performed via the Nokia Symbian 9.x. Devices Logical Plug-in.

> **Note:** Data on the device will not change in the acquisition process. No data and no applications are written to the device filesystem.

Acquired Data - Symbian 9.x

The program allows you to acquire the files stored in the memory of the device using the OBEX protocol.

The following types of data are acquired:

- File system (including Parsed Databases)
- Backup and Private data, including:
  - Logs
  - ToDo list
  - Calendar
  - Parsed Backup data
  - MailBox (including deleted messages)

- MMS History
- SMS History

<table>
<tr><th>Data Type</th><th>Data Format</th></tr>
<tr><td>Logs</td><td>This type of data contains grids with the information on outgoing and incoming calls and messages (including deleted logs) and the grid with configuration for log files. Each grid contains the following data:

Logs and Deleted logs grids:
ID
Event type
Direction
Contact Id
Number
Remote party
Subject
Date
Duration
Specific data
Config grid:
Parameter
Value</td></tr>
</table>

Data Type	Data Format
ToDo list	This type of data contains grids with the information on ToDo list acquired from the device and the last changes made to the list. Each grid contains the following data: ToDo list grid: • Description • Priority • Due date • Crossed out date • Creation date Last changes grid: • # • Description • Priority • Due date • Crossed out date • Creation date

Data Type	Data Format
Calendar	This type of data contains grids with the information on the list of calendar events acquired from the device and the last changes made to the list. Each grid contains the following data: Calendar grid: • Status • Description • Location • Type • Start date • Start time • End date • End time • Alarm time • Alarm days warning • Repeat type • Repeat specification • Repeat interval • Repeat forever • Repeat start date • Repeat end date • Creation date Last changes grid: • # • Status • Description • Location • Type • Start date • Start time • End date • End time • Alarm time • Alarm days warning

Data Type	Data Format
	• Repeat type • Repeat specification • Repeat interval • Repeat forever • Repeat start date • Repeat end date • Creation date
Mail box	This type of data contains grids with the information on Service Local MTM, SMS, MMS, Wap Push, Email SMTP, Email POP3, and deleted messages acquired from the device. Each grid contains the following data: Deleted messages grid: • Text • Number • Folder • Service • Date Stream SMS Header and Stream Schedule Data grids: • Property • Value
File System	This type of data contains binary nodes grouped by partition labels. Depending on the label, a partition contains the following data: • C: Internal phone memory • D:, E:. etc.: External memory cards (usually store music and multimedia files)
Parsed Databases	This type of data contains databases acquired from the device in binary nodes and grids with various data.

Data Type	Data Format
Backup data Split Backup data	This is data written into a special part of the memory by different applications. This data is shown in two forms: as it is read (backup data) and as it is stored, e.g. decrypted and split into files (split backup data).
Parsed Backup data	This is device backup data parsed into grids with various data.
MMS History	This type of data contains MMS messages acquired from the device in binary nodes.
SMS History	This type of data contains the SMS History grid with the information on SMS messages acquired from the device. The grid contains the following data: • Sender/Recipient • Text • Status • Type • Date and time (GMT) • Attachment

Supported Models - Symbian 9.x

Although all models available on the market today cannot be tested, any Nokia device that runs Symbian OS 9.x should work with the program.

Nokia Symbian 9.x Devices FAQ

Q: I cannot acquire SMS and email history. Why?

A: SMS and email history are not acquired for Symbian 9.1.

Q: It seems like not all the files from the filesystem are acquired. Why?

A: This may happen because of the specific device. Some system files may be locked and cannot be acquired.

COM Port Connection Settings

To define COM port connection settings:

1. Open the Symbian Dumpers subfolder of the program installation folder (you can find it in the Symbian Dumpers folder of the program installation directory).
2. Copy the **SymbianDumper.exe** file (for Symbian OS version 6.1 and higher) or the SymbianDumper6.0.exe file (for Symbian OS version 6.0) to an external memory card using a special Card reader.
3. Insert this external memory card into the device being investigated. Pay attention that the supporting file is not written to the device so it cannot damage the data stored on it.
4. Connect the device to the computer using a COM port cable.
5. On the **Home** page, click **Manual Plug-in Selection**.
6. On the **Plug-in Selection** page, select the Nokia Symbian OS (physical) plug-in.
7. On your Symbian device, navigate to the copied file (**SymbianDumper.exe** or **SymbianDumper6.0.exe**) and open it on the device.
8. In the opened window, select **SERIAL** for the connection type.
9. On the Connection Selection page, select the port via which the acquisition will be performed. Click the **Instructions** navigation link.
10. Once you have the instructions on the Instructions page, click **Start Acquisition**.
11. The data acquisition starts and its process is displayed on the Acquisition Progress page.
12. When the data acquisition finishes, the case is saved. Click **Finish**.

    Note: This process may take some time.

13. Disconnect your device from the computer.

IrDA Port Connection Settings

To define IrDA port connection settings:

1. Open the Symbian Dumpers subfolder of the DS installation folder (you can find it in the Symbian Dumpers folder of the program installation directory).
2. Copy the **SymbianDumper.exe** file (for Symbian OS version 6.1. and higher) or **SymbianDumper6.0.exe** file (for Symbian OS version 6.0.) to an external memory card using a special card reader.
3. Insert this external memory card into the device being investigated. Please note that the supporting file is not written to the device so it cannot damage the data stored on it.
4. Connect the Infrared adapter to your computer. Wait until the device is installed on your computer.
5. Start the program.
6. On the **Home** page, click **Manual Plug-in Selection**.
7. On the **Plug-in Selection** page, select the **Nokia Symbian OS (physical) plug-in**.
8. On your Symbian device, navigate to the copied file (**SymbianDumper.exe** or **SymbianDumper6.0.exe**) and open it on the device.

9. In the opened window, select IrDA for the connection type.
10. Connect the device to the computer using the IrDA connection (place the Infrared adapter next to the Infrared port of your Symbian device). You will see the notification item in the Windows taskbar if the device is connected.
11. On the **Connection Selection** page, select the port via which acquisition will be performed. Click the **Instructions** navigation link.
12. Once you have read the instructions on the Instructions page, click **Start Acquisition**.
13. Data acquisition starts, and its process is displayed on the Acquisition Progress page.
14. When data acquisition finishes, the case is saved. Click **Finish**.

    Note: This process may take some time.

15. Disconnect your device from the computer.

Bluetooth Connection Settings

To define Bluetooth connection settings

1. Open the **Symbian Dumpers** subfolder of the program installation folder (you can find it in the Symbian Dumpers folder of the program installation directory).
2. Copy the **SymbianDumper.exe** file (for Symbian OS version 6.1.) or **SymbianDumper6.0.exe** file (for Symbian OS version 6.0.) to an external memory card using a special card reader.
3. Insert this external memory card into the device being investigated. Please note that the supporting file is not written to the device so it cannot damage the data stored on it.
4. Connect the Bluetooth device to a USB port. Wait until the Bluetooth icon appears in the taskbar.
5. Right click the Bluetooth icon in the taskbar and select **Open Settings**.
6. In the **Bluetooth Settings** window, select the **Options** tab and select the **Allow Bluetooth devices to find this computer** checkbox. Click **Apply**.
7. Right click the Bluetooth icon in the taskbar and select **Add a Device**. In the newly-opened window, select the detected Symbian device and click **Next**.
8. Enter the code displayed by Windows into your Symbian device and press **OK**.
9. Wait until your device is completely connected. You will see the following page of the **Add a Device** wizard. Click **Close**.
10. On the Home page, click **Manual Plug-in Selection**.
11. On the **Plug-in Selection** page, select the **Nokia Symbian OS (physical) plug-in**.
12. Go to the **SymbianDumper.exe** (**SymbianDumper6.0.exe**) file on your external memory card on the phone and open it.
13. Select the Bluetooth connection (as shown on the following picture).
14. In the list of Bluetooth devices on the phone, select the name of the computer with the program installed and click **OK**.

15. Data acquisition starts, and its process is displayed on the Acquisition Progress page.
16. When data acquisition finishes, the case is saved. Click **Finish**.

    Note: This process may take some time.

17. Disconnect your device from the computer.

Data Acquisition - Nokia Symbian

Data acquisition is performed using the standard process. A device can be connected to the computer through the COM port, IrDA, or Bluetooth. We recommend that IrDA and Bluetooth connections only be used as a last resort as neither connection is secure. Data cables should always be your first choice as they are secure.

> **Note:** Physical acquisition of Nokia Symbian OS devices can only be performed via manual plug-in selection.

Pay attention to each connection process. You should define the correct settings for IrDA, Bluetooth, and COM port connection.

The acquisition is performed via the Nokia Symbian OS Physical Plug-in.

> **Note:** Data on the device will not change in the process of acquisition. No data and no applications are written to the device file system.

Acquired Data - Nokia Symbian

The Nokia Symbian OS Physical plug-in acquires the **Processes dump**.

A **Processes dump** includes all binary files used by the processes currently running on the device.

All data is acquired in the form of binary files and stored in folders whose names are the names of the currently running processes.

Supported Models - Nokia Symbian

The program allows you to perform physical acquisition of any devices that run Nokia Symbian OS up to version 8.x. Devices that run Nokia Symbian OS version 9.0 and higher are not supported.

Nokia Symbian OS Physical Acquisition FAQ

Q: I can't acquire data from this device. Why?

A: Check that you correctly set the Bluetooth, IrDA, or COM port connection for your device.

See also General Acquisition FAQ for more information.

Acquiring Data from a WebOS Based Device

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Preparing Device for Acquisition - WebOS

To prepare WebOS based device to the acquisition process:

1. Turn on the device.
2. Enter the main menu of the Palm device.

3. Enter the developer mode activation code. To do this, type `upupdowndownleftrightleftrightbastart`.



4. If you enter the code correctly, you'll see the developer mode application icon.



5. Enter the application and turn on developer mode.

6. After the device reboots, the developer mode will be on and you will be able to acquire the device.

   Note: After Palm Web OS is updated, the developer mode settings are reset. So the Developer Mode application can sometimes show that the developer mode is on while it is actually off.

7. Connect the device using the USB cable.

   Note: Use only the USB ports placed on the back of your system block.

8. Select the **Only charge** option of your device.

Data Acquisition - WebOS

Data acquisition of WebOS based devices is performed using the standard process, though it has to be prepared for the acquisition process and connected to the computer correctly.

The acquisition is performed via the WebOS Based Devices Logical Plug-in.

Acquired Data - WebOS

The program allows you to acquire the following information from the devices:

- File system text information
- Contacts
- E-mails
- SMS
- Memos
- Calendars
- Tasks
- Call history
- Accounts

Data is parsed and displayed in a grid.

Supported Models - WebOS

Although all models available on the market today cannot be tested, any device that runs WebOS should work with the program.

WebOS Devices FAQ

Q: I can't acquire data from this device. Why?

A: Check that your device has WebOS.

See also General Acquisition FAQ for more information.

Acquiring Data from PDAs

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

About Data Acquisition from PDA

The program allows you to acquire information from different types of PDA such as Palm, Windows Mobile, and Psion devices.

The following types of devices can be acquired:

- Psion 16/32 Bit Devices
- Palm OS Based Devices
- Windows Mobile Devices

The amount and the type of acquired data depends on the type of device.

Usually PDA plug-ins for the program allow you to acquire the following data:

- RAM
- ROM
- Databases Stored in the Memory

Connection Settings - Psion 16/32-bit devices

Before starting data acquisition, set the connection settings of your device (the connection to the serial cable and the proper speed).

Siena Series

Select **Menu > Special > Communications**.

In the dialog window, change settings to the following:

- **Use:** Serial Cable
- **Baud rate:** 19200

Series 3c

Select **Menu > Special > Communications**.

In the dialog window, change settings to the following:

- **Use:** Link Cable
- **Baud rate:** 19200

Series 5

Select the **Menu > Tool > Remote** link.

In the dialog window, change settings to the following:

- **Link:** Cable
- **Baud rate:** 19200

Note: For other Psion device settings, please read the instructions for your device.

Data Acquisition - Psion

Before starting data acquisition, set the connection settings of your device (the connection to the serial cable and proper speed must be set).

After that, data acquisition is performed using the standard process.

The acquisition is performed via the Psion 16/32 bit devices logical plug-in.

Note: Acquisition of Psion 16/32-bit devices can only be performed via manual plug-in selection.

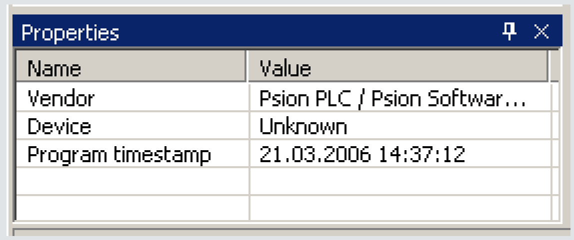
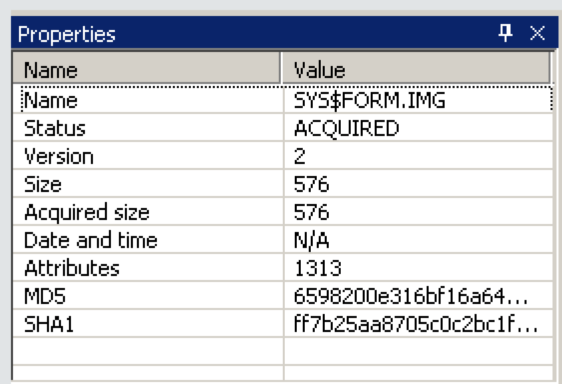
Acquired Data - Psion

The program allows you to acquire the file system from the device. Its structure depends on the group of Psion models to which your device belongs.

> **Note:** Some models of Psion devices lock ROM (disk C:) and RAM (internal disk). If they are locked, the program will not be able to acquire them. Locked disks are usually marked ABSENT in the menu of the device.
> All data is acquired in the form of binary nodes and is not parsed.

Type	Devices	Disks	Contents	Presence
Psion devices with SIBO (EPOC 16) OS	WorkAbout SERIES SIENA SERIES 3 SERIES 3a SERIES 3c SERIES 3MX	A:,B:	External disk	Can be absent if there are no external disks on the device.
		C:	ROM	Can be empty (depends on the type of the device).
		M:	RAM	Will be empty if a hard reset for a device was done.
Psion devices with EPOC 32 (ER3, ER5) OS.	SERIES 5 SERIES 5MX SERIES 7	C:	RAM	Will be empty if a hard reset for a device was done.
		Z:	ROM	
		(any letter)	External disk	Can be absent if there are no external disks on the device.

The properties of the acquired data can be seen in the Properties pane.

<table>
<tr><th>Node</th><th>Properties</th><th>Notes</th><th>Example</th></tr>
<tr><td rowspan="3">Device node</td><td>Vendor</td><td></td><td rowspan="3">
</td></tr>
<tr><td>Device</td><td>For Psion devices with SIBO (EPOC 16) OS, it will be defined only if RPC service is loaded.</td></tr>
<tr><td>Program timestamp</td><td></td></tr>
<tr><td rowspan="9">Binary node</td><td>Name</td><td></td><td rowspan="9">
</td></tr>
<tr><td>Status</td><td>May have the following value:
Acquired
Not acquired</td></tr>
<tr><td>Version</td><td></td></tr>
<tr><td>Size</td><td>The size of the acquired file defined in its properties on the device.</td></tr>
<tr><td>Acquired size</td><td>Actual size of the acquired file (it's usually equal to the Size value).</td></tr>
<tr><td>Date/Time</td><td></td></tr>
<tr><td>Attributes</td><td></td></tr>
<tr><td>MD5</td><td></td></tr>
<tr><td>SHA1</td><td></td></tr>
</table>

Psion 16/32-bit Devices FAQ

Q: I can't acquire data from this device. Why?

A: Check that connection settings are defined correctly.

See also General Acquisition FAQ for more information.

Q: The acquisition stops and the device stops responding. What do I do?

A: If this happens, restart the device and start the acquisition again. In some cases, you may need to do this multiple times before the proper acquisition process is completed. After restarting, please check the connection settings of the device thoroughly.

Data Acquisition - Palm OS

Physical acquisition is performed via the Palm OS Based Devices Physical Plug-in.

> **Note:** Some Palm devices (for example Treo 750) have the Window Mobile OS and must be acquired with the Windows Mobile/PocketPC logical plug-in or Windows Mobile 5-x/6-x physical plug-in.

To acquire data from the Palm:

1. Follow the steps of the standard process of data acquisition.
2. Before acquisition starts, you need to perform more steps.

- Put the device in console mode to acquire the Memory Image.
- To put the device in the console mode, do one of the following, then click **Continue**:
  - **If the device has the graffiti area:** Draw the following combination in the graffiti area: `ShortCut` (looks like a lowercase cursive l) `+ period + period +2`.
  - **If the device is a Handspring Visor using a serial connection:** Instead of the command shown above, use the `ShortCut` (cursive lowercase l) `+ period` and then hold the **Up** button while writing the number `2`. Devices using a USB connection do not require this additional step.
  - **If the device has no graffiti area (e.g., Treo 650):** Use the special key combination (e.g., `Search (Shift)+Sync Mode`). Please note that this combination may depend on the model of your device.

> **Note:** These instructions only work for Palm devices. The program should work with devices running the Palm OS made by other firms, but we can't guarantee it. Consult the instructions to your device to find out how to put it into the console mode.

- To acquire the Logical Image (Databases), put your device into the **Sync mode**. Press the **Sync** button on the cradle or activate the Sync mode through the screen dialog on the device, then click **Continue**.

3. If acquisition from a Palm device is being performed for the first time, the driver installation for it begins. This may lock the device.

   Note: If the device gets locked while acquiring Databases, press **Cancel**. If you are acquiring Memory and the device gets locked, restart the device (turn it off and then back on).

4. Acquisition starts.
5. There can be some files locked by the Palm OS on your device. If the program tries to acquire these files, it adds the file to the "black list" and stops acquisition. Files added to the black list are omitted on next acquisition. You have to repeat acquisition until all locked files are added to this list. After that, all unlocked files will be acquired without errors.
6. After acquisition finishes, click **Finish**.

Acquired Data - Palm OS

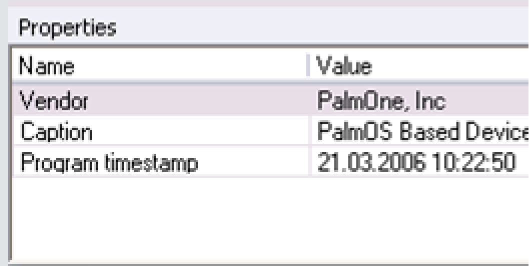
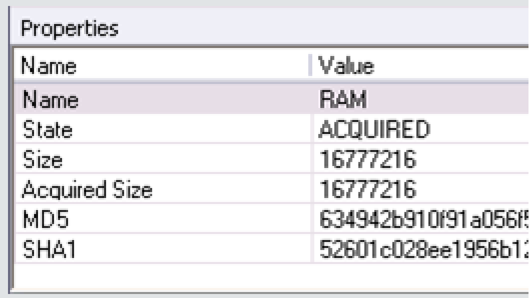
The program allows you to acquire the following information from the devices:

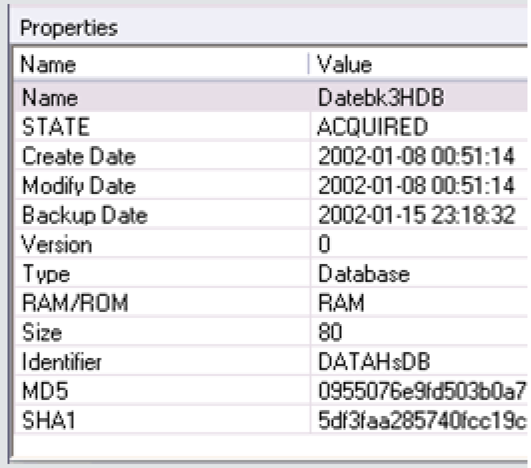
- Memory Images (ROM and RAM)
- Databases
- ROM Card Information (this information is read in the process of memory acquisition)

ROM Card Information contains the password field which will be filled if the device is locked by a password and runs Palm OS v4.0 or lower.

Some parts of data in databases will be parsed and displayed in grids form (MemoDB, AddressDB, DatebookDB, etc).

Properties of the acquired data can be seen in the properties window.

Node	Properties	Notes	Example
Device node	Vendor	This information is usually the same for all	 Properties Name | Value Vendor | PalmOne, Inc Caption | PalmOS Based Device Program timestamp | 21.03.2006 10:22:50
	Caption		
	Program timestamp		
RAM/ROM	Name		 Properties Name | Value Name | RAM State | ACQUIRED Size | 16777216 Acquired Size | 16777216 MD5 | 634942b910f91a056f SHA1 | 52601c028ee1956b1
	State	Acquired/Not Acquired.	
	Size	Actual size defined on the device.	
	Acquired Size	This size can be less than actual size.	
	MD5/SHA1	Calculated hash codes.	

Node	Properties	Notes	Example
Databases	Name		
	State	Acquired/Not Acquired/Parsed.	
	Create/Modify/backup dates		
	Version		
	Resource	Resource (resources or executable code)/Database (data).	
	Size		
	Identifier		
	MD5/SHA1	Hash codes.	

Supported Models - Palm OS

Any device running Palm OS should work with the program.

Palm OS Devices FAQ

Q: I can't acquire data from this device. Why?

A: Check whether your device has Palm OS. Some Palm devices (for example, Treo 750) have the Window Mobile OS and must be acquired by the Windows Mobile/PocketPC logical plug-in or Windows Mobile 5.x - 6.x physical plug-in.

See also General Acquisition FAQ for more information.

Q: Driver installation starts during acquisition. After driver installation, Palm does not acquire memory.

A: To resolve this problem, the user must reset the Palm device (use the hole on the back side of the device) before starting a new acquisition. It is strongly recommended that you acquire Databases before the Memory Image.

Q: I can't put the device into the console mode even when following the instructions given in the Data Acquisition topic. Why?

A: The given instructions are only suitable for devices made by Palm. EnCase Forensic should work with any Palm devices made by other firms, but it is not guaranteed. Consult the instructions for your device to find out how to put it into the console mode.

Q: I experience difficulties while acquiring ROM from devices with Palm OS 5.0. Why?

A: The problem is that some databases in the ROM are locked. When EnCase Forensic starts the acquisition and runs into a locked file, it freezes. You just need to restart the device and continue the acquisition. When this happens, the locked file will not be read again. It will be added to the list (its size will be near 70 - 80 bytes).

Q: The password is not acquired from the locked Palm. Why?

A: EnCase Forensic cannot acquire passwords from devices running versions of the Palm OS later than 4.0.

Q: When syncing the Palm device, the device reports "Unable to initiate HotSync operation because the port is used by another application". What's using the port?

A: Usually, this is caused by the device being placed into the console mode and not being reset. To fix this problem, soft reset the device using the pin hole on the back (usually labeled "Reset").

Q: The error message appears. The acquisition stops. Why?

A: There can be files locked by the OS on the device. These files cannot be acquired. They are added to the Black list and omitted during the following acquisitions. You have to repeat the acquisition process until all locked files from your device are added to the Black list. After this the acquisition is performed without errors.

Data Acquisition - Windows Mobile

Logical and physical acquisitions are performed using the standard process.

Logical acquisition is performed via the Windows Mobile Devices Logical Plug-in.

Physical acquisition is performed via the Windows Mobile 5.x – 6.x Devices Physical Plug-in.

Please note that, for logical acquisition, when a connection with the device is being established, the device will probably ask for a confirmation to write the .dll library into its memory. Please agree to this or else the connection won't be established.

> **Note:** Data acquisition can be done only with the help of a special .dll library which is written to the free space in the device memory. This guarantees that data stored in the device memory won't be lost.

Aquired Data - Windows Mobile

LOGICAL ACQUISITION - WINDOWS MOBILE

Logical acquisition allows you to acquire the following data in the form of binary nodes:

Acquired Data	Contents	Notes
Filesystem	The filesystem of the device including user files, system files, program files, and recovered deleted data.	The information from any external cards can be seen in the folder nodes named Storage Card, SD Card, CF Card, etc.
Databases	Databases stored on the device.	Windows Mobile 5.x and 6.x use removable databases. They cannot be read because they are locked by the device.
OS Registry	The information stored in the Windows Mobile register.	Information can be exported into XML format.
Logical Memory	The logical memory of the device.	Logical memory can be acquired from the processors ARM, MIPS, SH3, & SH4.

For Windows Mobile 5.x for Pocket PC Phone Edition, Windows Mobile 5.x for Smartphones, Windows Mobile 6.x Professional for Pocket PC, and Windows Mobile 6.x Standard for Smartphones, the following data is acquired in grid form:

Acquired Data	Contents	Fields Description
Call History	Call history of the device (outgoing, incoming, etc. call)	Call History: • **Name:** The name of the contact. • **Telephone Number:** The phone number of the contact. • **Telephone Number Type:** ◦ **w** - The work telephone number ◦ **h** - The home telephone number ◦ **m** - The mobile telephone number **Note:** The letter depends on the language of the phone. • **Caller ID type:** ◦ Unavailable ◦ Blocked ◦ Available • **Call Status:** ◦ Outgoing ◦ Missed ◦ Incoming • **Start Time (GMT):** The start time of the call • **End Time (GMT):** The end time of the call • **Duration:** Call duration in format `hh:mm:ss` • **Outgoing call:** ◦ **Yes** - Outgoing calls ◦ **No** - Incoming and missed calls • **Call Connected:** ◦ **Yes** - Call connected ◦ **No** - Busy ◦ **No answer**

Acquired Data	Contents	Fields Description
		• **Call ended:** ◦ **Yes** - Call ended ◦ **No** - Call dropped • **Roaming:** This parameter is "yes" for calls made while roaming, and "no" for "local" calls. ◦ **Yes** - Call made while roaming ◦ **No** - Local call • **Notes:** The file name of the associated Notes file if any.

Acquired Data	Contents	Fields Description
SIM Data	The Phonebook and the SMS history (including deleted SMS) stored on the SIM card **Note:** This data is acquired only if the SIM card is inserted and its phone functionality is turned on.	SIM Phonebook: • **Text:** The name of the contact • **Phone number:** The phone number of the contact • **Address type:** ○ International number ○ One national number ○ Network-specific number ○ Subscriber number (protocol-specific) ○ Alphanumeric address ○ Abbreviated number • **Numbering plan:** A type of numbering scheme used in telecommunications; for example, ISDN/mobile. SIM Messages (SMS history): • **Message:** SMS text. • **Phone number:** The number from which the SMS was sent. • **Receive time:** Time when the messages was received. • **Address type:** ○ International number ○ One national number ○ Network-specific number ○ Subscriber number (protocol-specific) ○ Alphanumeric address ○ Abbreviated number • **Numbering plan:** A type of numbering scheme used in telecommunications; for example, ISDN/mobile

Acquired Data	Contents	Fields Description
Pocket Outlook Items	Contacts information	Contacts: • **FirstName:** The first name for the contact • **LastName:** The last name for the contact • **MiddleName:** The middle name for the contact • **FileAs:** The filing string for a contact • **MobileTelephoneNumber:** The mobile or cellular telephone number for the contact • **HomeTelephoneNumber:** The home telephone number for the contact • **RadioTelephoneNumber:** The radio telephone number for the contact • **Email1Address:** The first e-mail address for the contact • **Birthday:** The birth date for the contact • **Anniversary:** The wedding anniversary date for the contact • **HomeAddressStreet:** The home street address for the contact • **HomeAddressCity:** The home city for the contact • **HomeAddressState:** The home state, department, or province for the contact • **HomeAddressPostalCode:** The home ZIP or postal code for the contact • **HomeAddressCountry:** The home country/region for the

Acquired Data	Contents	Fields Description
		contact • **BusinessFaxNumber:** The business fax number for the contact • **CompanyName:** The company name for the contact • **Department:** The department name for the contact • **OfficeLocation:** The office location for the contact • **PagerNumber:** The pager number for the contact • **BusinessTelephoneNumber:** The business telephone number for the contact • **JobTitle:** The job title for the contact • **Email2Address:** The second e-mail address for the contact • Spouse: The name of contact's spouse • **Email3Address:** The third e-mail address for the contact • **Home2TelephoneNumber:** The second home telephone number for the contact • **HomeFaxNumber:** The home fax number for the contact • **CarTelephoneNumber:** The car phone number for the contact • **AssistantName:** The name of contact's assistant • **AssistantTelephoneNumber:** The phone number for the contact's assistant • **Children:** The names of contact's children • **Categories:** The categories for

Acquired Data	Contents	Fields Description
		the contact • **WebPage:** The Web page for the contact • **Business2TelephoneNumber:** The second business telephone number for the contact • **Title:** The title for the contact • **Suffix:** The suffix for the contact name • **OtherAddressStreet:** The alternative street address for the contact • **OtherAddressCity:** The alternative city for the contact • **OtherAddressState:** The alternative state, department, or province for the contact • **OtherAddressPostalCode:** The alternative ZIP or postal code for the contact • **OtherAddressCountry:** The alternative country/region for the contact • **BusinessAddressStreet:** The business street address for the contact • **BusinessAddressCity:** The business city for the contact • **BusinessAddressState:** The business state for the contact • **BusinessAddressPostalCode:** The business ZIP or postal code for the contact • **BusinessAddressCountry:** The business country/region for the contact

Acquired Data	Contents	Fields Description
		• **Body:** The notes for the contact • **YomiCompanyName:** The Japanese phonetic rendering (Yomigana) of the company name for the contact • **YomiFirstName:** The Japanese phonetic rendering (Yomigana) of the first name for the contact • **YomiLastName:** The Japanese phonetic rendering (Yomigana) of the last name for the contact

Acquired Data	Contents	Fields Description
Pocket Outlook Items	Calendar information	Calendar • **Subject:** The description of the event • **Location:** Location of the event • **Categories:** Categories assigned to the event • **Start:** Start time of the event • **End:** Finish time of the event • **Duration:** Duration of the event • **IsRecurring:** ○ **Yes** - Recurring event ○ **No** - Non-recurring events • **RecurrencePattern:** The current recurrence pattern for the event. • **AllDayEvent:** ○ **Yes** - All day events ○ **No** - Events not set to all day • **BusyStatus:** User's availability during the event time • **Sensitivity:** Sensitivity for an event (normal or private) • **Body:** Ink notes or the message body accompanying the event • **Recipients:** A collection of recipients for an event that is a meeting • **MeetingStatus:** ○ **Yes** - Event is a meeting ○ **No** - Event is not a meeting • **ReminderSet:** ○ **Yes** - Event reminder set ○ **No** - Event reminder not set

Acquired Data	Contents	Fields Description
		• **ReminderSoundFile:** The name of the reminder sound file • **ReminderMinutesBeforeStart:** Time the reminder will play (reminder delay before event beginning) • **ReminderOptions:** The type of the reminder for the event • **BodyInk:** A binary representation of the event body

Acquired Data	Contents	Fields Description
Pocket Outlook Items	Tasks information	Tasks: • **Subject:** The description of the task • **Body:** The text of the notes accompanying the task • **Teamtask:** ◦ **Yes** - Task is a team task ◦ **No** - Task is not a team task • **IsRecurring:** ◦ **Yes** - Recurring task ◦ **No** - Not a recurring task • **RecurrencePattern:** The current recurrence pattern for the task • **Complete:** ◦ **Yes** - Task is complete ◦ **No** - Task is not complete • **Categories:** The categories assigned to the task • **StartDate:** Date when the task starts • **DateCompleted:** Date when the task is completed • **DueDate:** Date when the task is due • **Importance:** The importance of the task • **ReminderOptions:** The type of the reminder for the task • **ReminderSet:** ◦ **Yes** - Task reminder set ◦ **No** - Task reminder not set • **ReminderSoundFile:** The name of the reminder sound file • **ReminderTime:** Determines

Acquired Data	Contents	Fields Description
		when a reminder occurs before the start or due date of a task • **Sensitivity:** Sensitivity for a task (normal or private) • **BodyInk:** A binary representation of the task body

Physical Acquisition - Windows Mobile

Physical acquisition allows you to acquire data stored in the memory of the device and on the internal cards.

> **Note:** Data acquisition is performed with the help of a special DLL library, which is written to the free space in the device memory. This guarantees that data stored in the device memory won't be lost.

Acquired Data	Contents	Notes
Internal stores	ROM, the parsed FAT filesystem, and the binary file (Binary) that contains all unparsed data acquired from the device, including deleted data. The file containing Contacts is parsed.	All data stored in the device memory (storage) is acquired. But only the filesystem is parsed.
Memory cards	The parsed FAT filesystem and the binary file (Binary) that contains all unparsed data acquired from the device, including deleted data.	

The information about memory stores from which data was read (physical characteristics) can be seen in the Properties pane.

Supported Models - Windows Mobile

Logical acquisition should work with any device running Windows Mobile.

Physical acquisition should work with any device running Windows Mobile 5.x – 6.x.

Windows Mobile Devices FAQ

Q: I cannot acquire SIM data from my device. Why?

A: Make sure the SIM card is inserted in the device and the phone functionality of the device is turned on.

Q: I cannot acquire Call History, SIM data and Pocket Outlook items. Why?

A: Make sure you confirmed the DLL installation by tapping Yes on your device when the acquisition started. Also make sure that the security settings of your device allow internal applications to copy data to your device and to run unsigned applications on it.

Acquiring Data from GPS Devices

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Data Acquisition - Garmin GPS

Logical and physical acquisitions are performed using the standard process.

Logical acquisition is performed via the **Garmin GSP Logical Plug-in**.

Physical acquisition is performed via the **Garmin GSP Physical Plug-in**.

> **Note:** Physical acquisition can only be performed via a USB connection.

Do the following before starting the acquisition process:

- If you use a USB cable, make sure the required drivers are installed. The installation of these drivers is included in the Mobile Driver Pack.
- Turn off all external applications working with the Garmin GPS device.
- In the device settings, define **Garmin USB** as the connection protocol.

LOGICAL ACQUISITION - GARMIN GPS

Logical acquisition acquires the following data:

- Garmin Mass Storage Devices (Garmin nuvi): Device settings, Waypoints, Tracks, Routes, and Maps.
- Garmin Devices (eTrex, Rino, Edge, GPSMAP, etc.): Waypoints, Proximity waypoints, Tracks, Routes, Almanac, Maps, and Device properties.

Besides the standard case file containing the acquired data, the program allows you to create a GPS file. This file contains information about tracks, routes, and waypoints stored on the Device.

The GPS file (GarminGPS.gps) is placed as a sub-node of the device node and can be exported for future examination.

Garmin Mass Storage Devices

Data is read from the device as from a mass storage device. The acquired .gpx files are parsed and shown in the form of a grid:

<table>
<tr><th>Data Type</th><th>Notes</th><th>Data Format</th></tr>
<tr><td>Device settings</td><td>Device settings include two types of data:
Data type: Includes information about most device settings
Update file</td><td>For Data type data, a grid containing the fields:
Base name
File location
File path
Transfer direction
For update file, a grid containing the fields:
Part number
Description
Path
File name</td></tr>
</table>

Data Type	Notes	Data Format
Waypoints	Waypoints are sets of coordinates that identify a point in physical space.	A grid containing the fields: • Name • Position • Elevation (m) • Creation date/time (UTC) • Magnetic variation (deg) • Geoid height (m) • Comment • Description • Source of data • URL • Link • GPS symbol name • Classification • Number of satellites • HDOP • VDOP • PDOP • Time since last DGPS update (seconds) • DGPS station ID

Data Type	Notes	Data Format
Tracks	The actual path followed by a moving body	Three grids containing the fields: 1. Link ○ Text 2. Properties ○ Comment ○ Description ○ Source ○ Number ○ Type 3. Waypoints ○ Name ○ Position ○ Elevation ○ Creation date/time (UTC) ○ Magnetic variation ○ Geoid height ○ Comment ○ Source ○ URL associated ○ Text hyperlink ○ Symbol ○ Type (category) ○ GPS fix ○ HDOP ○ VDOP ○ PDOP ○ Time since last DGPS fix ○ DGPS station ID

Data Type	Notes	Data Format
Routes	Drawn by user course of travel.	Three grids: 1. URL ◦ Href ◦ Type ◦ Text 2. Optional ◦ Comment ◦ Description ◦ Source ◦ Number ◦ Type 3. Waypoints ◦ Name ◦ Position ◦ Elevation ◦ Creation date/time (UTC) ◦ Magnetic variation ◦ Geoid height ◦ Comment ◦ Source ◦ URL associated ◦ Text hyperlink ◦ Symbol ◦ Type (category) ◦ GPS fix ◦ HDOP ◦ VDOP ◦ PDOP ◦ Time since last DGPS fix ◦ DGPS station ID
Maps	Image file containing maps downloaded from the device and parsed.	Binary files

Note: The types and amount of acquired data depend on the type of device.

Garmin Devices (eTrex, Rino, Edge, GPSMAP, etc.)

The Garmin GPS Logical Plug-in acquires the following data from Garmin Devices (eTrex, Rino, Edge, GPSMAP, etc.):

- Waypoints
- Proximity waypoints
- Tracks
- Routes
- Almanac
- Maps
- Device properties

All data is acquired using the Garmin protocol.

Data Type	Notes	Data Format
Waypoints	Waypoints are sets of coordinates that identify a point in physical space.	A grid containing the fields: • Name • Attributes • Waypoint class • Waypoint color • Display option • Position • Attitude • Depth • Proximity distance • State • Country code • Waypoint symbol • Subclass

Data Type	Notes	Data Format
Proximity waypoints	Waypoints and the area around them.	A grid containing the fields: • Name • Attributes • Waypoint class • Waypoint color • Display option • Position • Altitude • Depth • Proximity distance • State • Country code • Waypoint symbol • Subclass
Tracks	The actual path followed by a moving body.	A grid containing the fields: • Text • Date/time

Data Type	Notes	Data Format
Routes	Drawn by user course of travel.	Three grids: 1. Links ◦ Route link class ◦ Subclass ◦ Identifier 2. Header ◦ Identifier 3. Waypoints ◦ Properties ◦ Attributes ◦ Waypoint class ◦ Waypoint color ◦ Display option ◦ Position ◦ Attitude ◦ Depth ◦ Proximity distance ◦ State ◦ Country code ◦ Waypoint symbol ◦ Subclass

Data Type	Notes	Data Format
Almanac	Data received from satellite.	A grid containing the fields: • Week number • Almanac data reference time • Clock correction coefficient (s) • Clock correction coefficient (s/s) • Eccentricity • Square root of semi major axis (a) (m** 1/2) • Mean anomaly at reference time (r) • Argument of perigee (r) • Right ascension (r) • Rate of right ascension (r/s) • Inclination angle (r) • Almanac health • Satellite ID
Maps	Image files containing maps downloaded from the device	Binary files

Data Type	Notes	Data Format
Device properties	These properties are shown in the Properties window after clicking on the device node.	A grid shown in the Properties window containing the fields: • Device current date • Device current position • Product ID • Software version • Other properties (Property #n) - number of this properties depend on the device characteristics

PHYSICAL ACQUISITION - GARMIN GPS

Physical acquisition acquires the Internal Memory Dump and Main Firmware from the Garmin GPS devices. Both files are acquired as binary files and are not parsed.

Supported Models - Garmin GPS

Although all models available on the market today cannot be tested, most Garmin models (including Garmin Nuvi, eTrex, Rino, Edge, and GPSMAP) with either USB or COM connection and Garmin Interface should work with the program.

Garmin GPS Devices FAQ

Q: I can't acquire data from this device. Why?

A: First, try the following:

- Make sure the drivers for the USB connection of your device are installed.
- Make sure you set Garmin USB as the connection protocol of your device.
- Make sure all external applications working with your device are turned off.

See also General Acquisition FAQ for more information.

Q: Connection is not established. Why?

A: Make sure that you’ve done the following:

- Set the connection protocol on the device to Garmin USB.
- Make sure the drivers for a USB connection are installed.

Q: The Almanac is not acquired. Why?

A: Some models of GPS devices need to have the Acquiring Satellites option turned **ON** to acquire the Almanac.

Data Acquisition - Tom Tom GPS

Data acquisition is performed using the standard process.

Acquisition is performed via the TomTom GPS Logical Plug-in.

> **Note:** Connect the device to the computer and make sure it is detected on the computer before you start the Acquisition Wizard.

Acquired Data - Tom Tom GPS

The TomTom GPS Logical Plug-in acquires GPS files from TomTom GPS devices.

Besides the standard case file containing the acquired data, the program allows you to create a GPS file. This file contains information about tracks, routes, and waypoints stored on the device. GPS files can be opened within the program and you can view information in Google Earth without exporting this file.

The GPS file (TomTomGPS.gps) is placed as a sub-node of the device node and can be exported for future examination.

The acquired files are parsed and shown in the form of a grid:

Data type	Notes	Data Format
Filesystem	Data stored in the device filesystem in the not parsed form.	Binary files

Data type	Notes	Data Format
Itineraries	Itinerary is planned route with destinations in addition to the final destination. A TomTom Itinerary is a file containing a list of locations that you can navigate. The locations are visited in the order that they appear in the list.	A grid containing the fields: • Longitude • Latitude • Comments • Flag • Other information
Contacts	Phone numbers stored in the TomTom address book.	A grid containing the fields: • Name • Phone number • Other information
Call Logs	Incoming and outgoing calls.	A grid containing the fields: • Name • Phone number • Other information
SMS History	Sent and Received SMS messages.	A grid containing the fields: • Name • Phone number • Message • Time • Type • Other information

Data type	Notes	Data Format
TomTom Configuration file	Map settings.	Home location, Favorite location, Recent locations and Other locations in grid form including the fields: • House number • Location type • Location description 1 • Location description 2 • Location description 3 • Location North • Location East • Road North • Road East • Location ID • Turn Point I North • Turn Point 1 East • Turn Point 2 North • Turn Point 2 East

Supported Models - Tom Tom GPS

Although all models available on the market today cannot be tested, most TomTom models should work with the program.

Acquiring Data from Feature Phones

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

About Feature Phone Plug-ins

The program allows you to acquire information from hundreds of models of feature phones. These non-smartphones are sometimes referred to as legacy phones or cell phones.

The following types of devices can be acquired:

- Alcatel
- CDMA Devices
- Kyocera CDMA
- LG CDMA
- LG GSM
- Motorola
- Motorola iDEN
- Nokia GSM
- Nokia TDMA
- Samsung CDMA
- Samsung GSM
- Sanyo CDMA
- Siemens
- Sony Ericsson
- ZTE

The types and amount of acquired data depend on the type of device. Usually, the feature phone plug-ins in the program allow you to acquire the following data:

- SMS History (including deleted SMS)
- Phonebook (both stored in the memory of the phone and on the SIM card)
- Call History (received calls, dialed numbers, missed calls, etc.)
- Datebook/Scheduler/Calendar/To-Do List (if any)
- Filesystem (consists of the system files, multimedia files, java files, etc.)

Data Acquisition - Alcatel

Data acquisition is performed using the standard process. Acquisition is performed via the Alcatel Logical Plug-in.

Acquired Data - Alcatel

The Alcatel Logical Plug-in acquires the following data:

Data type	Notes	Data Format
Call logs	History of call logs (dialed numbers, received calls etc)	A grid containing the fields: • ID • Name • Number • Date • Memory type
Phonebook	Numbers stored in the Phone memory and on SIM card	A grid containing the fields: • ID • Name • Mobile number • Memory type

Supported Models - Alcatel

Although all models available on the market today cannot be tested, any Alcatel model with a data connection should work with the program.

Data Acquisition - CDMA Devices

Data acquisition is performed using the standard process.

Physical acquisition is performed via the CDMA Devices Physical Plug-in.

> **Note:** Physical acquisition of CDMA devices can be performed only via manual plug-in selection.

Acquired Data - CDMA Devices

The program acquires the following data in the binary format:

- GUID properties
- NV Memory Dump
- Memory Dump (for all phone models except Samsung CDMA)

Supported Models - CDMA Devices

Although all models available on the market today cannot be tested, any CDMA model with a data connection should work with the program.

Data Acquisition - Kyocera CDMA

Data acquisition is performed using the standard process.

Acquisition is performed via the Kyocera CDMA Logical Plug-in.

> **Note:** Physical acquisition is performed via the CDMA Devices Physical plug-in.

Acquired Data - Kyocera CDMA

The program acquires the Filesystem using the BREW protocol. All data is acquired in the binary format.

Supported Models - Kyocera CDMA

Although all models available on the market today cannot be tested, any Kyocera CDMA model with a data connection should work with the program.

Data Acquisition - LG CDMA

Data acquisition is performed using the standard process.

Acquisition is performed via the LG CDMA Logical Plug-in.

> **Note:** Physical acquisition is performed via the CDMA Devices Physical plug-in.

Acquired Data - LG CDMA

The LG CDMA Logical Plug-in acquires the following data:

- SMS history
- Phonebook
- Filesystem
- Memo

- Call Logs
- Calendar

All data is acquired using the BREW protocol.

Data Type	Notes	Data Format
SMS history	SMS received and sent from the phone.	A grid containing the fields: • Text • State • Type • Sender/Recipient Number • Response/Reception Date • Subject
Phonebook	Numbers stored in the Phone memory.	A grid containing the fields: • Name • Phone1 • Phone2 • Phone3 • Phone4 • Phone5 • Email1 • URL • Memo • Email2 • Email3
Filesystem		
Users files (Java files, Multimedia, Sounds etc.)	The amount of data acquired depends on the model of the phone and its state.	Binary nodes
System files		
Memo		

Data Type	Notes	Data Format
Memo File Memo		A grid that contains one field: • Memo
	Call Logs	
Incoming Calls Outgoing Calls Missed Calls		A grid containing the fields: • Type of Call • Phone Number • Name • Entry Number in Phonebook • Duration (s) • Date
	Calendar	
Calendar File Exceptions File Calendar		A grid containing the fields: • Event ID • Description • Date Start • Repeat • Remind • Delay • Ringtone • Has Voice • Voice ID

Supported Models - LG CDMA

Although all models available on the market today cannot be tested, any LG CDMA model with a data connection should work with the program.

LG CDMA FAQ

Q: Data is not being read even though previous data was read without errors.

A: After acquiring data using the BREW protocol, you can't acquire data until you restart your mobile phone. In this case, turn off your mobile phone and then turn it back on.

Data Acquisition - LG GSM

Data acquisition is performed using the standard process.

Acquisition is performed via the LG GSM Logical Plug-in.

Acquired Data - LG GSM

The program acquires the following data:

- Phonebook
- SMS History
- Memos
- Filesystem (if present)
- Scheduler
- Call Logs
- ToDo list

All data is acquired using the AT Protocol.

Data Type	Notes	Data Format
Phonebook	Numbers stored in the Phone memory.	A grid containing the fields: • Name • Home number • Mobile number • Office number • Email • Memo
SMS history	Both sent and received SMS.	A grid containing the fields: • Text • State • Memory Type • Sender/Recipient Number • Response/Reception Date • SMS Center Number

Data Type	Notes	Data Format
Call Logs	History of call logs (dialed numbers, received calls etc).	A grid containing the fields: • Number • Type
ToDo		A grid containing the fields: • Text • Date • Status
Memos		A grid containing the fields: • Text • Date/time
Scheduler		A grid containing the fields: • Text • Date/time • Alarm date/time • Repeat
Filesystem		
Users files (Java files, Multimedia, Sounds etc)		Binary nodes
System files	The amount of data acquired depends on the model of the phone and its state.	

Supported Models - LG GSM

Although all models available on the market today cannot be tested, any LG GSM model with a data connection should work with the program.

LG GSM FAQ

Q: The phonebook is not acquired from the phone. Why?

A: It means that the support of your model has not been added to EnCase Forensic yet. Please send us your log files so that we are able to add support (the logs are located in `C:\Program Files (x86)\Guidance Software\Mobile Acquisition\logs` by default).

Installing Drivers -Motorola

If you use a USB data cable for connecting your phone, you should install the proper drivers.

The installation consists of three steps.

THE FIRST STEP: GENERAL INSTALLATION

Motorola drivers are included in the Driver Pack so you need to have it installed on your computer.

THE SECOND STEP: INSTALLATION UPON CONNECTION

The installation is performed when a new Motorola device is connected to the computer for the first time.

1. The Found New Hardware message will appear in the right bottom corner of the screen.
2. At the same time, the Found New Hardware wizard appears on the screen. Click the **Next** button.
3. The drivers search starts (the drivers are copied to the disk when the program is installed).
4. A caution message appears. Click the **Continue Anyway** button.
5. The installation finishes. Click the **Finish** button.
6. After this, it is recommended that you check whether the drivers are really installed. To do this, go to `Start\Settings\Control Panel\System\Hardware\Device Manager`. You should see the Mortorola USB Modem there.
7. This means the first step of the drivers installation has been performed successfully and you can acquire data through the AT modem now (Phonebook, Calendar, Calls History, and SMS history).

THE THIRD STEP: THE FINAL PART OF THE INSTALLATION.

This part of the installation is performed when a Motorola device tries to acquire the file system (or SMS and quick notes dump).

1. When you try to acquire this data for the first time, acquisition will be stopped and you will see an error message.

2. You will see a number of Found New Hardware messages in the tray notification area in the bottom-right corner of the screen, and then the installation of all these subdevices will begin. They will be installed one after another. Please note that this make some time. Sometimes there will be a pause between the installation of different subdevices.
3. During the driver installation process, information in the device manager window is changed. When the installation is totally finished, you should see all the interfaces under Motorola USB device in gray. They should not be marked with question or exclamation marks.
4. Reconnect or power-cycle the device and start acquisition.

> **Note:** Whenever you make selections, please leave the radio button selections as they are.

Data Acquisition - Motorola

Logical and physical acquisitions are performed using the standard process. When acquiring data via a USB connection, please pay attention to the process of drivers installation. Follow all the steps to acquire data without errors.

Please note that some devices, such as the Motorola VU 204, require the phone to be turned off before acquisition.

Logical acquisition is performed via the Motorola Logical Plug-in.

Physical acquisition is performed via the Motorola Physical Plug-in.

Acquired Data - Motorola

All data is acquired by the TCI Protocol.

LOGICAL ACQUISITION

Logical acquisition acquires the following data:

Data Type	Notes	Data Format	Protocol
Phonebook	Numbers stored in the Phone memory.	A grid containing the fields: • Location (Phone memory, Own number, Quick dial etc.) • Number • Name	AT protocol OBEX protocol (for some models)
SMS history	Both sent and received SMS.	A grid containing the fields: • Number • Status • Date/time • Text	TCI protocol
Call logs	Missed, received, and dialed calls list.	A grid containing the fields: • Name • Number • Direction (Received, Missed, Dialed)	AT protocol
File System			

Data Type	Notes	Data Format	Protocol
Users files (Java files, Multimedia, Sounds etc)	The amount of data acquired depends on the model of the phone and its state.	Binary nodes	TCI protocol (for GSM phones) BREW protocol (for CDMA phones) OBEX protocol (for some models of GSM phones)
System files			
Datebook		A grid containing the fields: • Title • Alarm timed • Alarm enabled • Start time/date • Duration • Alarm time/date • Repeat	AT protocol OBEX protocol (for some models)

The amount of acquired data depends on the model and state of the phone. The types of data listed above should be available; however, some of them can be empty or absent.

PHYSICAL ACQUISITION

Physical acquisition acquires the following data:

Data Type	Notes	Data Format
SMS History and quick notes dumps	SMS from Inbox and Outbox. Quick notes.	For SMS, a grid containing the fields: • Creator number • Sender number • Recipient number • Text • Date/Time • Dump (hyperlink that allows you to view dump corresponding to the SMS in the Text and Hex viewers) For Quick notes, a grid containing the fields: • Text • Date/Time • Dump (hyperlink that allows you to view dump corresponding to the Quick notes in the Text and Hex viewers)
Calls logs	Incoming and outgoing calls.	A grid containing the fields: • Name • Number • Date/Time • Duration
Security information	Restored security information from the phone, including security codes, IMEI, and more.	Data is shown in grid form.

Note: Quick notes can only be extracted by physical acquisition. Logical acquisition does not acquire them.

Supported Models - Motorola

Although all models available on the market today cannot be tested, any Motorola model (other than iDen models which have their own plug-in) with a data connection should work with the program.

Motorola FAQ

Q: I can't acquire data from this device. Why?

A: When acquiring data through a USB connection, make sure the process of drivers installation is performed correctly.

See General Acquisition FAQ for more information.

Q: Data is not being read even though previous data was read without errors. Why?

A: After acquiring data by the TCI or BREW protocol, you can't acquire data until you restart your mobile phone. In this case, turn off your mobile phone and then turn it on.

Q: After the acquisition, the phone does not connect.

A: The device may be locked. Restart it.

Data Acquisition - Motorola iDEN

Logical and physical acquisitions are performed using the standard process. Please pay attention to the following when working with Motorola iDEN phones:

- Phones without SIM cards cannot be acquired.
- If acquisition from the current device has just been performed, you should reconnect or restart it if you want to acquire data again.
- If you use a USB cable, make sure that the iDEN p2k Device – iDEN USB Modem drivers are installed.

Logical acquisition is performed via the Motorola iDEN Logical Plug-in.

Physical acquisition is performed via the Motorola iDEN Physical Plug-in.

LOGICAL ACQUISITION - MOTOROLA IDEN

Logical acquisition acquires the following data from the phone SIM card:

Data Type	Notes	Data Format	Protocol
Phonebook	Numbers stored on the SIM Card	The grid containing the fields: • ID • Number • Name	Direct protocol
SMS history	Both sent and received SMS stored on the SIM Card	The grid containing the fields: • ID • Date/Time • Text	Direct protocol
Filesystem			
SIM card filesystem	Information stored on the SIM card (GSM, iDEN and Telecom folders)	Binary nodes	RSS protocol

The amount of acquired data depends on the model and state of the phone. The types of data listed above should be available; however, some of them can be empty or absent.

PHYSICAL ACQUISITION - MOTOROLA IDEN

Physical acquisition acquires the following parts of memory from the phone:

Data	Notes	Protocol
RAM	Random Access memory	Data is read using the I55 protocol and Direct.
Flex	Mobile's OS	
User Data space	The amount of memory for any custom user data, such as pictures, ringtones, Java files etc.	

Please note that data stored on the SIM card is not acquired.

Note: For Falkon models, the file system data is parsed.

Supported Models - Motorola iDEN

Although all models available on the market today cannot be tested, any Motorola iDEN model with a data connection should work with the program.

Motorola iDEN FAQ

Q: Data is not read. The Can't establish flashStarp connection error message appears. Why?

A: This may happen because the phone is not charged. Restart the phone, recharge it, and try again.

Data Acquisition - Nokia GSM

Logical and physical data acquisition procedures are performed using the standard process.

Logical acquisition is performed via the Nokia GSM Logical Plug-in.

Physical acquisition is performed via the Nokia GSM Physical Plug-in.

Nokia drivers for new Nokia phone models (Nokia N97, Nokia 6700, etc.) and older ones are included in the Driver Pack.

Acquired Data - Nokia GSM

Usually the amount of acquired data depends on the model and state of the phone. The types of data listed above should be available, however, some of them can be empty or absent.

LOGICAL ACQUISITION

Logical acquisition acquires the following data using the FBUS protocol:

Data Type	Description	Data Format
Phone Book		

Data Type	Description	Data Format
Phone	Numbers stored in the phone memory.	A grid containing the fields: • Name • General number • Home number • Mobile number • Work number • Fax number • Email 1 • URL • Caller Group ID • Caller Group Name • Caller Group Logo • Postal, Note • Date • Ringtone ID
SIM card	Numbers stored on the SIM card.	
	SMS	
User folders		A grid containing the fields: • Name • Text • Picture • Type • State • Memory type • Format • Validity period • Sender/Recipient name • Re-sponse/Reception date • Default Recipient name • SMS Centre number • SMS Centre name • Reply

Data Type	Description	Data Format
Call logs		
Missed Calls Received Calls Dialed Numbers Unknown		A grid containing the fields: • Name • No. • Caller Group ID • Date/Time
Calendar		
Call Memo Meeting Birthday Reminder		A grid containing the fields: • Start date • End date • Alarm date • Silent alarm date • Recurrence • Text • Location • Phone
ToDo List		
Sorted by priority (High, Low etc)		A grid containing the fields: • Due date • Complete Status • Alarm date • Silent alarm date • Text • Private • Category • Contact ID • Phone
Logos		
Start up logos		Binary nodes (image nodes)
WAP		

Data Type	Description	Data Format
WAP settings (unparsed)		A grid containing the fields: • Location • Title • URL
WAP bookmarks		
Profiles		A grid containing the fields: • Location • Format • Validity • Name • Default number • Number
GPRS access points		A grid containing the fields: • Position • Active • Name • URL
Notes		A grid containing one field: • Text
Chat Settings		
MMS Settings		
SyncML Settings		
FM Station		
	File System	
Java files Multimedia Sounds Other files	The amount of acquired data depends on the model of the phone and its state.	Binary nodes

PHYSICAL ACQUISITION

Physical acquisition acquires EEPROM memory using the FBUS protocol. The following data will be parsed:

Data Type	Description	Data Format
Permanent Memory	Not parsed blocks of data stored in the EEPROM.	Binary nodes
Phonebook	Parsed numbers stored in the phone memory.	A grid containing a number of fields that depends on the amount of data stored in the device's memory. Possible fields: • Name • General Phone Number • Mobile Phone Number • Home Phone Number • Work Phone Number • Fax Number • Note • Email • URL • Post Address • Caller Group ID

Data Type	Description	Data Format
SMS History	SMS messages parsed from the memory flash including Inbox, Outbox, Archive, Template (User templates) folders. These folders can include several subfolders Read, Unread, Sent, Unsent, Deleted, Template and Subfolders created by Users.	A grid containing a number of fields that depends on the amount of data stored in the device's memory. Possible fields: • Message type • SMS text • Picture number (the picture with the corresponding name is stored separately) • Sender phone number • Service phone number • Date/Time • Combined message ID (means that message includes several parts) • Part serial number (number of the part of the message Combined message ID) • Total number of parts (total number of parts in the message Combined message ID)
Call logs		

Data Type	Description	Data Format
Missed, Incoming, Outgoing	Restored from the phone memory Call logs.	A grid containing a number of fields that depends on the amount of data stored in the device's memory. Possible fields: • Name • General Phone Number • Mobile Phone Number • Home Phone Number • Work Phone Number • Call Date
Calendar		
Call, Memo, Meeting, Birthday, Reminder		A grid containing a number of fields that depends on the amount of data stored in the device's memory.

The following phone properties stored in the EEPROM are parsed and shown in the Properties viewer:

- Serial Number
- Product code
- Basic product code
- Module code
- Hardware version
- Security Code
- ICC-ID

Supported Models - Nokia GSM

Although all models available on the market today cannot be tested, most Nokia models with a data connection should work with the program.

Data Acquisition - Nokia TDMA

Data acquisition is performed using the standard process. Acquisition is performed via the Nokia TDMA Logical Plug-in.

Acquired Data - Nokia TDMA

The program acquires the Phonebook which is displayed in the form of a grid containing the fields:

- Name
- General
- Location

Supported Models - Nokia TDMA

Although all models available on the market today cannot be tested, most Nokia TDMA models with a data connection should work with the program.

Data Acquisition - Samsung CDMA

Data acquisition is performed using the standard process.

Acquisition is performed via the Samsung CDMA Logical Plug-in.

Note: Physical acquisition is performed via the CDMA Devices Physical plug-in.

Acquired Data - Samsung CDMA

The Samsung CDMA Logical plug-in acquires the following data:

Data Type	Comments	Data Format
Phone Book		

Data Type	Comments	Data Format
Contacts	Numbers stored in the phone memory.	A grid containing the fields: • Name • Phone number 1 • Phone number 2 • Phone number 3 • Phone number 4 • Phone number 5 • Speed dial number • Email • URL • Caller Group ID • Date/Time • Number Label • Secrecy • Memory Type
Calendar		
	Tasks for the day.	A grid containing the fields: • Text • Start date/time • Finish date/time • Creation date/time • Alarm
SMS History		
	Received and sent SMS stored in the phone.	A grid containing the fields: • Address • Message • Date/Time
File System		

Data Type	Comments	Data Format
Java files	The amount of data acquired depends on the model of the phone and its state.	Binary nodes
Multimedia		
Sounds		
Other files		
Call History		
	Calls made from the device.	A grid containing the fields: • Name • Mobile Number • Date/Time • Call Type
Notes		
	Written records.	Field content in the grid depends on data stored in each individual device.
ToDo History		
	Information from the ToDo list.	A grid containing the fields: • Text • Due Date/Time • Alarm Date/Time • Priority

All data is acquired by the BREW protocol.

The amount of acquired data depends on the model and state of the phone. The types of data listed above should be available; however, some of them can be empty or absent.

Supported Models - Samsung CDMA

Although all models available on the market today cannot be tested, any Agere, Sysol, SGH-C1xx, and SGH-A800 models with a data connection should work with the program.

Samsung CDMA FAQ

Q: My device is not detected. How can I fix this?

A: Try downloading and installing the Kies application. It contains all necessary drivers for Samsung devices:
http://www.samsung.com/in/support/usefulsoftware/KIES/JSP#versionInfo.

Q: When recovering audio from a Samsung CDMA phone, there are files that are unplayable with various types of media players after exporting. What do I do?

A: Samsung CDMA devices store *.wav files in their internal QCP format. For playing such wav files, you should use QUALCOMM's PureVoice Player.

LOGICAL DATA ACQUISITION - SAMSUNG GSM

Acquisition is performed using the standard process.

Acquisition is performed via the Samsung GSM Logical Plug-in.

It is strongly recommended that you enter the PIN code on your device before starting an acquisition. Otherwise, some data (SMS, Calendar, Call Logs, and Phone Book) from the device might not be acquired.

VLSI DEVICES PHYSICAL ACQUISITION

Data acquisition is performed using the standard process. Before acquisition, turn off the phone, remove the battery, and insert it back again. After that, connect the phone to the computer with the cable.

Acquisition is performed via the Samsung GSM Physical Plug-in.

> **Note:** Don't unplug the cable until acquisition completes.

CONEXANT PHYSICAL ACQUISITION

Data acquisition is performed using the standard process. Before acquisition, turn off the phone, remove the battery, and insert it back again. After that, connect the phone to the computer with the cable.

Acquisition is performed via the Samsung GSM Physical Plug-in.

SYSOL DEVICES PHYSICAL ACQUISITION

Data acquisition is performed using the standard process. Before acquisition, turn off the phone, remove the battery, and insert it back again. After that, connect the phone to the computer with the cable.

When the phone is connecting to the computer (the Connection page appears), press the **Power** button on your cell phone for 1-2 seconds. This activates the connection to the phone. Be careful that the phone does not turn on. If it turns on, you should disconnect it and start the acquisition procedure from the beginning (this can be tricky and may require many attempts). Then click the **Next** button on the Complete Acquisition window.

Acquisition is performed via the Samsung GSM Physical Plug-in.

AGERE DEVICES PHYSICAL ACQUISITION

Data acquisition is performed using the standard process. Before the acquisition, turn off the phone, remove the battery, and insert it back again. After that, connect the phone to the computer with the cable. Turn on the phone and wait until it loads to the desktop or to the Enter Your PIN screen. If it is a flip-phone, it should remain closed.

Acquisition is performed via the Samsung GSM Physical Plug-in.

LOGICALLY ACQUIRED DATA - SAMSUNG GSM

The program acquires the following data:

Data Type	Notes	Data Format
Phone Book		

<table>
<tr><th>Data Type</th><th>Notes</th><th>Data Format</th></tr>
<tr><td>Phone</td><td>Numbers stored in the phone memory.</td><td rowspan="2">A grid containing the fields:
• Name
• General number
• Home number
• Mobile number
• Work number
• Fax number
• Email 1
• URL
• Caller Group ID
• Caller Group Name
• Caller Group Logo
• Postal, Note, Date
• Ringtone ID</td></tr>
<tr><td>SIM card</td><td>Numbers stored in the SIM card.</td></tr>
<tr><td colspan="3">Calendar</td></tr>
<tr><td>Scheduler</td><td></td><td>A grid containing the fields:
• Start date
• End date
• Alarm date
• Silent alarm date
• Recurrence
• Text
• Location
• Phone</td></tr>
<tr><td colspan="3">SMS History</td></tr>
</table>

<table>
<tr><th>Data Type</th><th>Notes</th><th>Data Format</th></tr>
<tr><td>Inbox</td><td></td><td rowspan="2">A grid containing the fields:
• Text
• State
• Memory type
• Sender/Recipient name
• Response/Reception number
• Response/Reception date
• SMS Centre number</td></tr>
<tr><td>Outbox</td><td></td></tr>
<tr><td colspan="3">File System</td></tr>
<tr><td>Java files</td><td rowspan="4">The amount of data acquired depends on the model of the phone and its state.</td><td rowspan="4">Binary nodes</td></tr>
<tr><td>Multimedia</td></tr>
<tr><td>Sounds</td></tr>
<tr><td>Other files</td></tr>
</table>

The amount of acquired data depends on the model and state of the phone. The types of data listed above should be present, however, some of them can be empty or absent.

Generally, all data is acquired by the AT protocol. The OBEX protocol is used for some models.

VLSI

The program acquires only EEPROM.

CONEXANT

The program acquires only EEPROM from Conexant generation phones and the file system from Conexant 2 generation phones.

SYSOL

The program acquires three types of data: RAM, EEPROM, and NAND.

AGERE

The program acquires only EEPROM (with PIN Code extraction) and flash file system.

Samsung GSM FAQ

Q: My device is not detected. How can I fix this?

A: Try downloading and installing the Kies application. It contains all necessary drivers for Samsung devices: http://www.samsung.com/in/support/usefulsoftware/KIES/JSP#versionInfo.

Q: I can't acquire the SMS, Calendar, Call Logs and Phonebook from this device. Why?

A: Some Samsung phones don't allow you to acquire these features until the PIN code is entered.

Q: The acquisition has finished but the phone won't turn back on. What happened?

A: This happens because it takes time for the phone to switch off from the service mode. Try pressing the power button for varying lengths of time. If the phone still doesn't turn on (some firmware versions don't have a software reset), you should disconnect and then reconnect the battery and try again.

Q: The phone does not switch to the service mode. Why?

A: This happens when the buffers are filled with trash data. In this case, turn the phone off and then on or, if this does not help, disconnect and reconnect the battery.

Data Acquisition - Sanyo CDMA

Data acquisition is performed using the standard process.

Acquisition is performed via the Sanyo CDMA Logical Plug-in.

> **Note:** Physical acquisition is performed via the CDMA Devices Physical plug-in.

Acquired Data - Sanyo CDMA

The program acquires the following data by the BREW protocol:

Data Type	Note	Data Format
Phone Book	Numbers stored in the phone memory.	A grid containing the fields: • Name • Numbers 1-7 • Email 1-2 • URL • Address • Memo • Secret
SMS history	Incoming and outgoing SMS.	A grid containing the fields: • Phone number • Callback • Date • Priority • Status • Message
Call history	Incoming, missed and outgoing calls.	A grid containing the fields: • Number • Date • Name
ToDo list	Information from the ToDo list.	A grid containing the fields: • ToDo • Priority
File System	User data and system files.	Files in the binary format.

Supported Models - Sanyo CDMA

Although all models available on the market today cannot be tested, any Sanyo CDMA model with a data connection should work with the program.

Logical Acquisition - Siemens

Data acquisition is performed using the standard process.

Acquisition is performed via the Siemens Logical Plug-in.

Physical Acquisition - Siemens

Data acquisition is performed using the standard process.

Acquisition is performed via the Siemens Physical Plug-in.

Before acquisition, turn off the phone, remove the battery, and insert it back again. After that, connect the phone to the computer with the cable.

Please note that physical acquisition of Siemens devices can only be performed via manual plug-in selection and you need to define the exact model of the phone.

When the phone is connecting to the computer, the Information screen appears.

Press the **Power** button of your mobile phone for 1-2 seconds. This activates the connection to the phone. Make sure the phone stays turned off. If it turns on, you should disconnect it and re-start the acquisition process.

The phone should not ask you to insert a SIM card.

Click **Start Acquisition**.

LOGICAL ACQUISITION - SIEMENS

Logical acquisition acquires the following data:

Data Type	Note	Data Format	Protocol
Phone Book			
SIM card	Numbers stored on the SIM Card.	A grid containing the fields: • Name • Mobile Number	AT protocol
Phone	Numbers stored in the phone memory.		
Own numbers	The phone's own numbers.		
SMS History			

Data Type	Note	Data Format	Protocol
Inbox		A grid containing the fields: • Text • State (Sent or Read) • Memory type (Phone or SIM card) • Sender/Recipient number • Response/ Reception Date • SMS centre number	AT protocol
Outbox			
Call logs			
Missed calls		A grid containing the fields: • ID • Name • Mobile number • Date/time	AT protocol
Received calls			
Dialed numbers			
Last dialing numbers	Last dialed numbers from the SIM card and phone memory.		
Fixed dialed	SIM Fix Dialing, restricted phonebook.		
File System			

<table>
<tr><th>Data Type</th><th>Note</th><th>Data Format</th><th>Protocol</th></tr>
<tr><td>Java files</td><td rowspan="4">The amount of the acquired data depends on the model of the phone and its state.</td><td rowspan="4">Binary nodes</td><td rowspan="4">OBEX protocol</td></tr>
<tr><td>Multimedia</td></tr>
<tr><td>Sounds</td></tr>
<tr><td>Other files</td></tr>
<tr><td colspan="4">Calendar</td></tr>
<tr><td>To Do List</td><td></td><td>A grid containing the fields:
Due date
Complete status
Completed
Start date
Text
Priority
Category
Contact ID
Phone</td><td>OBEX protocol</td></tr>
<tr><td colspan="4">Phone Book OBEX</td></tr>
<tr><td>Phone</td><td>Numbers stored in the phone’s memory with more detailed information.</td><td>A grid containing the fields:
Name,
Mobile number,
Home number,
Work number,
E-mail,
Address,
Group,
Organization,
Birthday</td><td>OBEX protocol</td></tr>
</table>

Usually the amount of acquired data depends on the model and state of the phone. The types of data listed above should be present but sometimes some of it can be empty. Some old models of phones do not support the standard version of the OBEX protocol. Data read by the OBEX protocol in these phones cannot be acquired.

PHYSICAL ACQUISITION - SIEMENS

Physical acquisition acquires data stored in the memory of the mobile phone. After acquisition, it is automatically parsed and represented as a set of binary nodes. Even the information usually represented as a grid (Phonebook, SMS, etc.) is acquired in the form of binary files.

The following data will be acquired:

- Phone book
- SMS History (Inbox, Outbox)
- Java Files
- Multimedia Files
- User Settings
- Other Files Stored in the Memory

The amount of acquired information depends on the model of the phone and its state.

Siemens FAQ

Q: The filesystem cannot be not read although previously data was read without errors. Why?

A: In some models of Siemens phones (A56i,C56, etc.), after the acquisition of the Calendar, the file system cannot be read. In this case, turn off the device and then turn it back on. After this, the file system can be acquired.

Data Acquisition - Sony Ericsson

Data acquisition is performed using the standard process.

Acquisition is performed via the Sony Ericsson Logical Plug-in.

Acquired Data - Sony Ericsson

The Sony Ericsson plug-in acquires the following data:

Data Type	Notes	Data Format	Protocol
Phone Book			

Data Type	Notes	Data Format	Protocol
Phone	Numbers stored in the phone's memory and on the SIM card.	A grid containing the fields: • Name • Mobile Number • Home Number • Work Number • E-mail • URL • Group • Organization • Birthday • Address	OBEX protocol (if it is supported) or AT protocol
SMS			
Inbox		A grid containing the fields: • Text • State (Sent or Read) • Memory Type (Phone or SIM card) • Sender/Recipient Number • Response/Reception Date • SMS Center Number	AT Protocol
Outbox			
Call Logs			

Data Type	Notes	Data Format	Protocol
Missed Calls		A grid containing the fields: • ID, • Name, • Mobile Number, • Date/Time	AT Protocol
Received Calls			
Dialed Numbers			
Last Dialed Numbers	Last dialed numbers from the SIM card and phone memory.		
Fixed Dialing	SIM Fix Dialing, restricted phonebook.		
File System			
Java Files	The amount of data acquired depends on the model of the phone and its state.	Binary Nodes	OBEX protocol
Multimedia			
Sounds			
Other Files			
Calendar			
To Do List		A grid containing the fields: • Start Date, • End Date, • Alarm Date, • Silent Alarm Date, • Recurrence, • Text, • Location, • Phone	OBEX Protocol
Anniversary			
Scheduler			
Call			

Usually the amount of acquired data depends on the model and state of the phone. Parts of the data listed above should be available but sometimes some of them can be absent.

Some old models of phones do not support the standard version of the OBEX protocol. Data read by the OBEX protocol from these phones cannot be acquired.

Supported Models - Sony Ericsson

Although all models available on the market today cannot be tested, any Sony Ericsson model with a data connection should work with the program.

Data Acquisition - ZTE

Data acquisition is performed using the standard process.

Acquisition is performed via the ZTE Logical Plug-in.

Acquired Data - ZTE

The program acquires the following data:

Data Type	Notes	Data Format
Phone Book	Numbers stored in the phone memory.	A grid containing the fields: • Memory type • Mobile number • Name • Mobile number 2 • Work number • Home number • City • Country • E-mail • E-mail 2 • Fax number • Postcode • State • Street
File System	User data and system files.	Files in the binary format

Supported Models - ZTE

Most ZTE devices should work with the program.

Acquiring Data from SIM Cards

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process. This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Data Acquisition - SIM Cards

Data acquisition is performed using the standard process.

Logical acquisition is performed via the SIM Card Reader Plug-in.

If the card is locked by a PIN code, you will be asked to enter it before acquisition starts.

> **Note:** You only have 3 attempts to enter the PIN code. After that, the PUK code will be requested. After you enter the right PUK, the SIM card PIN will be reset to 0000.

Acquired Data - SIM Cards

The program acquires data stored on the SIM card.

Data like SMS and phone numbers (Abbreviated Dialing Numbers and Service Dialing Numbers) is acquired in two formats: parsed and unparsed.

Parsed data is represented as grids showing information in a way suitable for analyzing. Each SMS message is shown in a separate grid which includes all information about the message.

- Abbreviated dialing numbers
- Access control class
- Access Overload Class
- Accumulated call meter
- ACM maximum value
- Administrative data
- Administrator Root Public Key
- AMPS Usage Indicators
- Automatic Answer for eMLPP Service
- Barred Dialing Numbers
- Broadcast control channels
- Call Count
- Capability configuration parameters
- Cell Broadcast Message Identifier for Data Download
- Cell broadcast message identifier range selection
- Cell broadcast message identifier selection
- Ciphering key Kc
- Comparison Method Information
- Co-operative Network List
- CPBCCH Information

- Extension1
- Extension2
- Extension3
- Extension4
- Fixed dialing numbers
- Forbidden PLMNs
- GPRS Ciphering key KcGPRS
- GPRS location information
- Group ID
- Group Identifier Level 1
- HPLMN search period
- HPLMN Selector with Access Technology
- ICC Identification
- Image
- Initial Paging Channel
- International Mobile Subscriber Identity
- Investigation Scan
- Language preference
- Last number dialed
- Location information
- MExE Service table
- Mobile Identification Number
- MSISDN
- Negative/Forbidden SID List
- Network's Indication of Alerting
- Operator controlled PLMN Selector with Access Technology
- Operator Root Public Key

- Phase identification
- PLMN selector
- Positive/Favored SID List
- Price per unit and currency table
- Registration Threshold
- RPLMN Last used Access Technology
- RPLMN Last used Access Technology
- RUIM ID (for CDMA RUIM)
- Service Dialing Numbers
- Service Provider Name
- SetUpMenu Elements
- Short message status reports
- Short messages
- SIM Electronic Serial Number (for SIM cards)
- SIM service table (for SIM cards)
- SMS parameters
- SMS status
- SoLSA Access Indicator
- SoLSA LSA List
- System ID
- Third Party Root Public key
- User controlled PLMN Selector with Access Technology
- Voice Broadcast Service Status

• De-personalization Control Keys • Emergency Call Codes • Enhanced Multi-Level Preemption and Priority • Extended Capability configuration parameters • Extended Language preference		• Voice Broadcast Service • Voice Group Call Service Status • Voice Group Call Service

Most of the data listed above can be found in the file system folder in a parsed format.

> **Note:** Usually the amount of acquired data depends on the model and state of the phone.

For more information about data stored on the SIM card and abbreviation explanations, see International Journal of Digital Evidence.

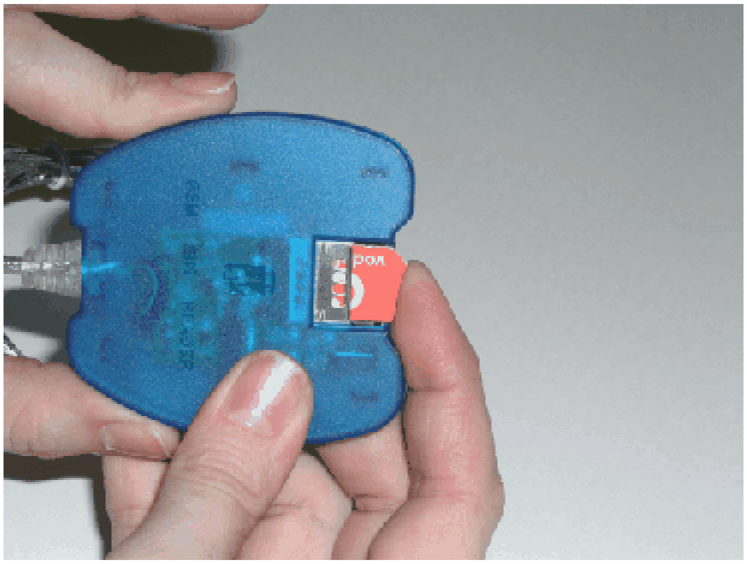
Besides the data listed above, the system and provider-specific data which wasn't included in any specification, if found on the device, will be acquired from GSM SIM and CDMA RUIM cards.

Supported Models (Card Readers) - SIM Cards

The SIM Card Reader Logical plug-in supports data acquisition from both the GSM and CDMA SIM cards.

The following types of card readers are supported:

- COM SIM card reader



- USB SIM card reader



- PC\SC USB card reader



- Mass storage card reader



- All-in-one card reader



> **Note:** There may be problems acquiring some SIM cards with mass storage SIM card reader when running Windows 7 or later.

SIM Card Reader FAQ

Q: I cannot acquire data from the SIM Card. Why?

A: First, try the following:

- Make sure your SIM card reader is supported, connected to your PC, and is not damaged.
- Thoroughly read the instructions on how acquisition should be performed.

See also General Acquisition FAQ for more information.

Q: After acquiring information from the SIM card from a Siemens phone, I see the last symbol in the names in the phone book is invalid. Why?

A: Siemens phones save the name of the group to which the number belongs in the last character. That's why it cannot be parsed.

Q: Can I enter a PUK instead of PIN code to unlock a SIM card?

A: Yes. You can enter an invalid PIN code 3 times and then enter the right PUK. After that, the PIN code will be reset to 0000.

Q: I cannot acquire a SIM card on Windows 8/10, although everything worked fine on Windows 7. Is there a way to fix this?

A: By default, the latest available driver for SIM card readers is automatically installed on Windows 8/10. You can try selecting an older driver.

To select a driver for a SIM card reader:

1. Open the Windows Device Manager.
2. In the device list, right click your SIM card reader and click Update Driver Software in the context menu.
3. The Update Driver Software window opens.
4. On the **How do you want to search for driver software** page, click **Browse** my computer for driver software.
5. On the **Browse** for driver software on your computer page, click **Let me pick from a list of device drivers on my computer**.
6. On the **Select the device driver** you want to install for this hardware page, select the required driver in the list and click **Next**.
7. The driver installation process starts.
8. After the driver is installed, click **Close**.

Acquiring Data from Memory Cards/Mass Storages/e-Readers/Portable Devices

With the forensic process, it is important to note that, with embedded systems such as smart devices, some data must be written to the device in order to communicate with it. Depending on the type of device, the data that is written will change. However, in order to follow the principles of forensics, the data that is written is documented and noted as part of the process.

This process is repeatable with multiple devices and is considered forensically sound. In each section, the details of the process can be found. The methods used by the program are designed to write the minimal amount of data to the device to allow for a forensically stable data acquisition.

Data Acquisition - Memory Cards

Data acquisition is performed using the standard process.

Physical acquisition is performed via the Memory Card Plug-in.

Acquired Data - Memory Cards

The Memory Card Physical plug-in performs a bit-stream acquisition of the memory card filesystem. The filesystem is parsed and its content is shown in the form of binary files.

Supported Cards - Memory Cards

Although all memory cards available on the market today cannot be tested, any memory card with the FAT filesystem (CompactFlash Card, MicroSD, Secure Digital Card, etc.) should work with the program.

Data Acquisition - Portable Devices

Data acquisition of portable devices is performed using the standard process.

Logical acquisition is performed via the Portable Device Logical Plug-in.

Acquired Data - Portable Devices

The program acquires the user media content (image, audio, and video files) of a portable device and any other files to which the device OS gives access.

Supported Models - Portable Devices

The program supports acquisition from a variety of portable devices, such as mobile phones, digital cameras, portable media players, and Kindle e-book readers.

Portable Device FAQ

Q: I cannot acquire data from the Memory Card. Why?

A: Check that your card reader is supported, connected to your PC, and is not damaged.

See also General Acquisition FAQ for more information.

Q: There are a number of empty folders acquired from the device. What are they?

A: A folder acquired from the device may be empty in the following cases:

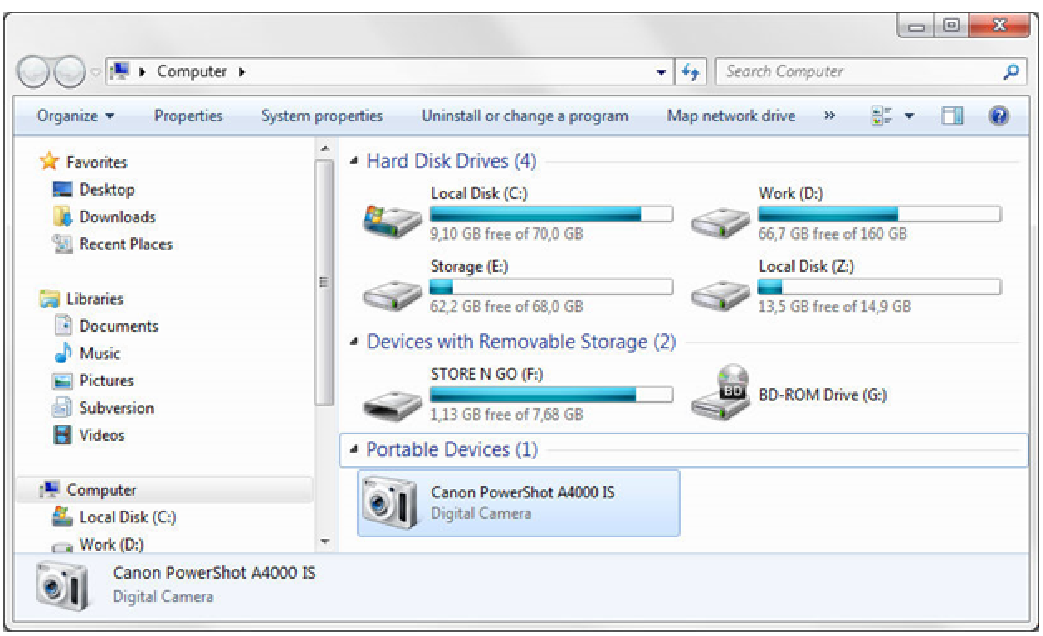
- The folder is empty on the acquired device.
- The files in the folder are locked by the device OS.

Q: What is the difference between acquiring a device with its native plug-in and Portable Device plug-in?

A: Portable Device plug-in guarantees to acquire only the user media content from the device. Generally, a native plug-in allows to acquire more data. For example, many devices store media files, such as music and photos, within the area of the device that can mount as media for acquisition while the user data is stored in other areas only accessible with acquisition by the native plug-in.

Q: How do I know that my device belongs to portable devices?

A: If you have a portable device, after connecting it to your computer it will be displayed under the Portable Devices group in Computer (This PC in Windows 8 and 10).



Data Acquisition - Mass Storage

Data acquisition is performed using the standard process.

Physical acquisition is performed via the Mass Storage/eReader Physical Plug-in.

> **Note:** It can take a long time to acquire data from high capacity mass storage devices.

Acquired Data - Mass Storage

The Mass Storage/e-Reader Physical plug-in performs a bit-stream acquisition of the mass storage and e-Reader device filesystems. The filesystem is parsed and its content is shown in the form of binary files. The items marked with a red X contain recovered deleted data.

Importing Data

Importing is the process of adding data received by other programs to the case.

You can import the following types of data:

- Data from Cellebrite UFED cases
- Data from iOS backup files (including encrypted backups)
- Data from RIM BlackBerry backup files (including encrypted backups)
- GPS and KML files
- Device backup data from Tarantula cases
- GSM tower information

Importing Data from Cellebrite UFED Cases

EnCase Forensic allows importing data from the cases created in Cellebrite UFED.

To import Cellebrite UFED case data:

1. Do one of the following:
   - Click **Add Evidence** on the Home screen, then select **Acquire from File** on the Add Evidence screen.
   - Select **Add Evidence > Acquire Mobile > Acquire from File** from the top toolbar.

2. Complete the fields and select the output folder in the Output File Settings dialog and click **OK**.
3. The Import Wizard opens. Select **Cellebrite UFED Case** and click **Next**.
4. Click **Browse** and browse to the file to be imported (*.ufd or *.xml). Click **Finish**.

5. The data importing starts and a new Import stored mobile data task is added to the Tasks pane, where you can view its general progress.
   The progress is also displayed on the Importing File Process page of the Import wizard.
6. If the importing process finishes correctly, you will see the last page of the Import wizard. Click **Finish**.
7. Data is imported to the case.

Importing Data from iOS Backup Files

EnCase Forensic allows you to import the following types of iOS backup data:

- iPhone OS 1.x – 11.0.x backup
- iPhone OS 3.x – 10.2 encrypted backup

Encrypted data can be imported from iOS 11 devices if you have the encryption key.

EnCase Mobile Investigator allows you to parse the following data from iPhone backups:

Data Type	Parsed Data	Parsed Recovered Data
Address Book Images	✓	✕
Calendar	✓	✓
Call History	✓	✓
Cell Locations	✓	✓
Contacts	✓	✓
Contact Properties	✕	✓
Cookies	✓	✕
Dynamic Text	✓	✕
Messages (SMS, MMS, and iMessages)	✓	✓
Mac Address	✓	✕
Mail Accounts	✓	✕
Maps Bookmarks	✓	✕

Data Type	Parsed Data	Parsed Recovered Data
Maps Directions	✓	✕
Maps History	✓	✕
Notes	✓	✓
Keychain Data (passwords and account info)	✓ (encrypted backups only)	✕
Safari History	✓	✕
Safari Suspend State	✓	✕
Safari Bookmarks	✓	✕
Voicemail	✓	✕
WiFi Locations	✓	✓
YouTube Bookmarks	✓	✕
Device Properties	✓	N/A

In addition, encrypted iOS backups include extracted authentication data, which can be used to import data from cloud-based services.

To import data:

1. Do one of the following:
    - Click **Add Evidence** on the Home screen, then select **Acquire from File** on the Add Evidence screen.
    - Select **Add Evidence > Acquire Mobile > Acquire from File** from the top toolbar.
2. Complete the fields and select the output folder in the Output File Settings dialog and click **OK**.
3. The Import Wizard opens. Select **iPhone Backup** and click **Next**.
4. Click **Browse** and browse to the file to be imported. Click **Finish**.

> **Note:** To import iPhone files, load the Manifest.plist file to make sure you have all the supporting files in the backup folder intact. If you load an *.mdbackup file for iPhones, you will not need any supporting files.

5. If the backup file is encrypted, you will be asked to enter a password. Enter a password and click **Next**.
6. The data importing starts and a new Import stored mobile data task is added to the Tasks pane, where you can view its general progress.
   The progress is also displayed on the Importing File Process page of the Import wizard.
7. If the importing process finishes correctly, you will see the last page of the Import wizard. Click **Finish**.
8. Data is imported to the case.

Importing Data from RIM BlackBerry 1.x - 7.x Backup Files

EnCase Forensic allows you to import RIM BlackBerry 1.x – 7.x backup data.

To import data:

1. Do one of the following:
   - Click **Add Evidence** on the Home screen, then select **Acquire from File** on the Add Evidence screen.
   - Select **Add Evidence > Acquire Mobile > Acquire from File** from the top toolbar.
2. Complete the fields and select the output folder in the Output File Settings dialog and click **OK**.
3. The Import Wizard opens. Select **RIM Blackberry Backup** and click **Next**.
4. Click **Browse** and browse to the file to be imported. Click **Finish**.

> **Note:** To import BlackBerry backup files, load the backup file with the *.ipd extension to make sure you have all supporting files in the backup folder intact.

5. If the backup file is encrypted, you will be asked to enter a password. Enter a password and click **Next**.
6. The data importing starts and a new Import stored mobile data task is added to the Tasks pane, where you can view its general progress.
   The progress is also displayed on the Importing File Process page of the Import wizard.
7. If the importing process finishes correctly, you will see the last page of the Import wizard. Click **Finish**.
8. Data is imported to the case.

Importing Data from RIM BlackBerry 10.x Encrypted Backup Files

EnCase Forensic allows you to import RIM BlackBerry 10.0.x – 10.3.1 encrypted backup data.

> **Note:** A BlackBerry 10 backup may be incomplete. To make sure all data from the device is present in a backup, make a complete backup of the device if you have access to it.

EnCase Mobile Investigator parses the following types of data from RIM BlackBerry 10 backup data:

- Calendar
- Contacts
- Call Logs
- SMS
- Notes

Additionally, the following application data is parsed:

- BlackBerry Messenger
- Evernote
- Skype
- WeChat
- WhatsApp

To import data:

1. Do one of the following:
    - Click **Add Evidence** on the Home screen, then select **Acquire from File** on the Add Evidence screen.
    - Select **Add Evidence > Acquire Mobile > Acquire from File** from the top toolbar.
2. Complete the fields and select the output folder in the Output File Settings dialog and click **OK**.
3. The Import Wizard opens. Select **RIM Blackberry Backup** and click **Next**.
4. Click **Browse** and browse to the file to be imported. Click **Finish**.
5. You will be asked to enter a password. Enter a password and click **Next**.

    > **Note:** An active Internet connection is required to obtain a decryption key from the RIM BlackBerry server after you enter the password.

6. The data importing starts and a new Import stored mobile data task is added to the Tasks pane, where you can view its general progress.
   The progress is also displayed on the Importing File Process page of the Import wizard.

   Note: When importing BlackBerry 10 encrypted backup, EnCase Mobile Investigator performs the backup decryption procedure that requires at least 3 times more space on the system disk than the size of the backup.

7. If the importing process finishes correctly, you will see the last page of the Import wizard. Click **Finish**.
8. Data is imported to the case.

Importing GPS and KML Files

EnCase Mobile Investigator allows you to view information stored on GPS devices (waypoints, tracks, etc.) on Open Street maps. The information is obtained from *.gps files, which can be received from devices during acquisition. You can also import map files (*.gps and *.kml files) to the E3 mobile data case and view them within Open Street maps.

To import map files:

1. Do one of the following:
   - Click **Add Evidence** on the Home screen, then select **Acquire from File** on the Add Evidence screen.
   - Select **Add Evidence > Acquire Mobile > Acquire from File** from the top toolbar.

2. Complete the fields and select the output folder in the Output File Settings dialog and click **OK**.
3. The Import wizard opens. Select the **GPS and KML Map** and click **Next**.
4. Click **Browse** and browse to the file to be imported. Click **Finish**.
5. The data importing starts and a new Import stored mobile data task is added to the Tasks pane, where you can view its general progress.
   The progress is also displayed on the Importing File Process page of the Import wizard.
6. If the importing process finishes correctly, you will see the last page of the Import wizard. Click **Finish**.
7. Double-click a *.gps or *.kml file in the Data View pane (it is placed as a subnode of the device node).
8. In the Data View pane, the Open Street Viewer opens. The information received from the device is displayed in a tree-view structure on the right side of the pane.
9. Select the location (waypoint, route, etc.) in the tree view to navigate to it in the Open Street Viewer.

Importing Tarantula Data

EnCase Forensic allows importing device backup data created in Tarantula.

To import Tarantula data:

1. Do one of the following:
    - Click **Add Evidence** on the Home screen, then select **Acquire from File** on the Add Evidence screen.
    - Select **Add Evidence > Acquire Mobile > Acquire from File** from the top toolbar.
2. Complete the fields and select the output folder in the Output File Settings dialog and click **OK**.
3. The Import wizard opens. Select **Tarantula** and then click **Next**.
4. Click **Browse** and navigate to the file to be imported (*.xml). Click **Finish**.
5. The data importing starts and a new Import stored mobile data task is added to the Tasks pane, where you can view its general progress.
   The progress is also displayed on the Importing File Process page of the Import wizard.
6. If import finishes correctly, you will see the last page of the Import wizard. Click **Finish**.
7. Data is imported to the case.

Importing Cloud Data

Cloud data importing is the process of obtaining user data from cloud-based services via the Internet using user account credentials or authentication tokens extracted from the following sources:

- Logically acquired Android OS devices (devices already rooted or rootable by EnCase Forensic)
- Imported encrypted iTunes backups (from devices with iOS 7.x and higher)

Note: The support of extraction from logically acquired iOS devices will be added in the future releases.

Using the Cloud Data Import wizard, you can obtain data from online services, such as:

- Facebook
- Gmail
- Google Drive
- Twitter
- Amazon Alexa

Extracting Authentication Data File

An authentication data file is a binary file that contains authentication tokens, web cookies, and saved user credentials. The authentication data file is automatically created in case data in the following situations:

- When you perform a logical acquisition of an Android OS device (devices already rooted or rootable by EnCase Forensic).
- When you import an encrypted iTunes backup (from devices with iOS 7.x and later).

After acquisition/importing, you will find the authentication data file in the Authentication Data folder in the device/backup root folder. The file name contains the name of the device from which it was extracted and the time of extraction.

This file is used to obtain data from the corresponding cloud-based service accounts via the Cloud Data Import wizard.

In the current version of EnCase Forensic , authentication data for the following services is extracted:

- Amazon Alexa
- Facebook
- Gmail
- Google Drive
- Google Locations
- Twitter

> **Note:** For iOS backups, Gmail and Google Drive authentication data can be extracted only if the user logged in to these services via a mobile browser.

Importing Cloud Data

EnCase Forensic allows you to import data from cloud-based services in one of the following ways:

- Using authentication data file extracted from logically acquired Android OS data or from imported encrypted iTunes backups
- By manually entering credentials from the user's account

> **Note:** User credentials for cloud-based services can sometimes be found in parsed iOS keychains (primarily in the General Password Data and Web-form Passwords grids).

To import data from cloud-based services:

1. If you have an authentication data file in your case, export it to your computer.
2. Do one of the following:
    - Click **Add Evidence** on the Welcome screen, select **Acquire from Cloud** in the Acquire Smartphone category, and click **OK**.
    - In the top navigation bar, click **Add Evidence > Acquire Mobile > Acquire from Cloud**.
3. The Output File Settings window appears. Fill out the information on both tabs and click **OK**.
4. The Cloud Data Import Wizard opens and the Accounts and Sources page is displayed.
5. If necessary, in the **Cloud investigation name** field, define the name under which imported data will appear in the case.
6. Do one of the following:
    - To add accounts from an authentication data file, click **Add Auth Data File** and select the previously exported authentication data file.

        Note: Some account logins may be unknown until the corresponding accounts are authenticated.

    - To add accounts manually, click **Add Account**, and define a Data Source (service) from which data must be imported, Account/Login, and Password.
7. Select the checkboxes of the accounts from which you want to import data and click **Authenticate**.
8. The authentication of the selected accounts starts and its progress is displayed on the Authentication Process page.

    Note: During authentication, account credentials and tokens are sent directly to the corresponding authentication servers and are not saved anywhere.

9. After the authentication process finishes, click **Continue**.
10. On the Data for Importing page, the list of successfully authenticated accounts will be displayed.
11. Do the following (if necessary) and click **Import Data**:
    - Select the **Select custom date range for time related data** checkbox and select the date range for which time-related data (messages, calendar, etc.) from selected accounts must be imported.

        Note: Data that does not have timestamps, such as contacts or images, will be imported to the full extent.

- Select accounts in the accounts table and then select which data must be imported from each account. To import all data from an account, select a checkbox next to it; to import no data, clear a checkbox next to it.

12. The cloud data importing starts and a new **Import data from cloud** task is added to the Tasks pane, where you can view its general progress.
13. The progress is also displayed on the Importing Progress page of the Cloud Data Import Wizard.
14. After the importing finishes, click **Finish**.

Imported Cloud Data

The Cloud Data Import wizard allows you to import the following data from cloud-based services:

Service Name	Imported Data	Additional Information
Amazon Alexa	User name User ID User email Recording time Summary Audio Device type	• **User name** is the user's first and last name. • **User ID** is the user's username for Amazon. • **User email** is the email address associated with the user's Amazon account. • **Recording time** is the date and time of recorded voice activity. The format is `YYYY-MM-DD HH:MM:SS`. • **Summary** is Alexa's interpretation of the voice activity. • **Audio** is the audio file for the voice activity. • **Device type** is the type of Alexa device that has been synched with Amazon. For example, the Amazon Echo an Echo Dot are both Alexa devices.
Facebook	Profile Information Friends News Feed Notifications Conversations Photo Albums (including actual pictures)	Facebook contains photos and message attachments. Depending on the number and the size of attachments, importing may take some time.

Service Name	Imported Data	Additional Information
Gmail	Inbox Sent Mail Draft Trash Spam Chats	Gmail messages include email attachments. Depending on the number and size of attachments, importing may take some time.
Google Drive	User storage files Files shared with a user	During importing, all files from selected folders are downloaded. This may take a while.
Google Locations	Saved Places Timeline	
Twitter	Profile Information Conversations Posted Tweets	

Cloud Data Importing FAQ

Q: How long can a token stay valid?

A: It depends on the type of the service. Token lifespan may be unlimited or may be just half an hour.

Q: Can I view the passwords from extracted authentication data?

A: No, the passwords are stored in an encrypted format and cannot be viewed.

General Acquisition FAQ

Q: My device is not displayed on the Home page. Why?

A: Some devices require special actions to be performed so that the device is detected. Start the acquisition wizard or see the FAQ for the corresponding device for more information. Additionally, some devices, like Psion 16/32-bit devices, cannot be automatically detected and must be acquired via manual plug-in selection (see the description of data acquisition process for the corresponding device).

Q: The type of device connection is not shown in the Connections Selection page of the Acquisition Wizard. Why?

A: One of the following may cause the problem:

- The PC port is locked by another program (close the programs which may be locking the port).
- The port of the cell phone is locked. Restart the phone (if this doesn't help, take out the battery and re-insert it).
- If a USB Connection is not shown, it may be because the drivers of the USB port are not installed.
- Some devices require special actions to be performed so that the device is detected. Click the troubleshooting link in the bottom of the Home page of the Acquisition Wizard or see the FAQ for the corresponding device for more information.

Q: Data acquisition won't start. An error message appears. Why?

A: The error message contains the description of the error and advice on what to do to solve the problem.

Your problem can be caused by the following:

1. Phone problems:
   - Check whether the device is charged.
   - Check whether the device is turned on (for logical acquisition) or, in some cases, turned off (for physical acquisition).
   - Read the instructions on how the acquisition for your device should be performed.

2. Problems with the cable:
   - Check whether the cable is connected to the device and to the computer properly.
   - Check whether the cable is compatible with your device.
   - Check whether the cable working.

3. Problems with the software:
   - Check whether the drivers for the USB port are installed (if you use a USB connection).

- Check that your port is not locked by any other program.
- There may be issues with Microsoft ActiveSync on some computers. Try uninstalling it if you have problems with acquisition.

4. Manual selection problems:
    - Try acquiring the device via automatic detection.
    - Check whether the manufacturer was selected correctly.
    - Check whether the device model was selected correctly.
    - Check whether the connection type was selected correctly (make sure you are selecting the correct port).
    - Check whether the drivers for the USB port are installed (if you use a USB connection).

If you can't find the problem, try doing the following:

1. Disconnect the cable from the computer as well as from the phone and then reconnect it again.
2. Turn on/off the phone and turn it off/on again and reload the phone.
3. Pull out the battery from the phone and insert it back again.

If the problem persists, contact Technical Support.

Q: The Data Acquisition Process starts correctly but, in the middle of the acquisition, an error appears. Why?

A: Your problem can be caused by the following:

- Bugs in the device’s operating system. In this case, try reloading your device.
- The phone ran out of power. Charge the phone and try again.
- The connection was broken. Maybe the cable was unplugged accidentally or has a loose connection.

Q: Some data that should be acquired is not acquired. Why?

A: Bugs in the device's operating system may cause this error. Try reloading your device. You can also try acquiring each type of data separately.

Q: I have X phone from Y manufacturer and I get the message that the phone isn't supported. Why isn't this particular phone supported yet?

A: There are currently thousands of models of phones out on the market, and new phones are being introduced every day. It is impossible for Guidance Software to support and test every make and model that is available. We are trying to add support for all the most popular model phones on the market and are adding more model support every month. If you have a model that isn't currently supported, please follow these instructions for submitting log files, and we'll work on adding support for your phone as soon as possible:

1. Once the device is connected properly to your computer, begin the acquisition.
2. After the acquisition finishes (timeout, error, problem), close EnCase Forensic .
3. Browse to the Logs folder (by default, it is `C:\Program Files (x86)\Guidance Software\Mobile Acquisition\logs`).
4. In the Logs folder, find the log that corresponds to the manufacturer of the phone you tried to acquire. For each plug-in, there are two logs present: *.txt and *.dump (for example, plugin.psion_logical.txt and plugin.psion_logical.dump).
5. Rename the log file to include the model number of the phone. For example motorola_log.txt should be renamed to motorola_c331_log.txt.
6. Check the size of the log file to ensure that information from the acquisition was captured. If the file is a zero byte file, try acquiring the phone again.
7. Once the log file has been renamed, place the file in a .zip archive to ensure that, when we receive the file, the data is unaltered. Some mail servers alter the data contained in *.txt files. Sending it in a zip file ensures that this does not happen.
8. Contact Technical Support.

Q: EnCase Forensic shuts down after the first 10 minutes of acquisition. Why?

A: Chances are that you are running a personal firewall on the same machine that you are using EnCase Forensic on. The personal firewall will block the communication between your device and the computer. Disable the firewall and start the acquisition process again. This will most commonly occur when you work with a Windows Mobile 5 device.

Q: How can I check that the Prolific drivers for my device are installed correctly?

A: If you want to check whether the Prolific drivers were properly installed, do the following:

1. Connect your device to the computer using a USB cable.
2. Go to **Start > Settings > Control Panel > System > Hardware > Device Manager**.
3. There, in the list of ports, you should see a new COM port that will have a name similar to *USB virtual serial port (COM 15)*. Its name will change depending on the kind of device that is connected and the system parameters.

Q: What should I do if the drivers for my device are not installed?

A: Drivers for most supported types of devices are included in the Mobile Driver Pack, which you can download from www.guidancesoftware.com. If none of the drivers installed from the Mobile Driver Pack work, try searching the web or contacting our support staff.

Q: What kinds of devices are currently supported with EnCase Forensic ?

A: We currently support a broad range of Sony-Ericsson, Motorola, LG, Nokia, Samsung, Siemens, Sanyo, Kyocera, ZTE, iPhone, and Google Android phones as well as PDAs running the Palm OS through 5.4, WebOS, Windows CE/Pocket PC/Mobile 5.0 (and some 6.0 devices) and earlier, Windows Phone 7 & 8, RIM BlackBerry, Symbian 6.0, 7.0, 8.0, & 9.0, EPOC 16/32 (Psion devices) Operating Systems, Garmin and TomTom GPS devices, GSM and CDMA SIM cards, media cards, and Windows Portable Devices.

Q: Does EnCase Forensic support the acquisition of SIM cards that are located in many GSM and even some CDMA phones?

A: Yes, EnCase Forensic supports full acquisition of GSM and CDMA SIM cards from all manufacturers.

Q: I acquired a GSM phone and later on I acquired the same GSM phone and I had more results the second time around. What is causing this?

A: The first time you performed acquisition, the SIM card in the phone hadn't fully initialized yet. When you power a phone with a SIM card, it takes anywhere from one to three minutes for the phone to fully initialize the SIM card. If you perform acquisition before the SIM card is done initializing, EnCase Forensic won't be able to acquire all the data located on the phone. The solution to this is to wait one to three minutes before starting your acquisition.

Q: I have EnCase Mobile Investigator and a pile of cell phones but I can't find the correct data cable to connect the phone to the computer. Where can I find the correct data cables?

A: EnCase Mobile Investigator includes a toolbox of cables and hardware. You'll not only receive cables that work on most phones on the market today, you'll receive a StrongHold Bag, power adapters, a remote charger, and more. Guidance Software also offers the Mobile Field Kit for a complete portable forensic solution that allows you to perform acquisitions, analysis, and reporting in the field. For more information on our Electronic Evidence Examiner Toolbox, please visit www.guidancesoftware.com. As new software support is added, we also add new cable connection support.

Q: The Electronic Evidence Examiner Toolbox doesn't include the cable I need. What now?

A: Guidance Software will be happy to help you locate the cables you require. Please contact Technical Support.

Q: Can EnCase Forensic recover deleted text messages from phones and the SIM card?

A: Yes. EnCase Forensic can recover deleted SMS text messages from SIM cards and phones. However, as with any deleted data, there is a possibility that some data recovered will be in fragments and incomplete or that the data has been entirely overwritten. This all depends on when the message was deleted and what other information had been written to the phone or SIM card. Deleted data recovery can also depend on whether the plug-in(s) for your device support deleted data recovery.

Q: Can EnCase Forensic acquire graphics/pictures from cell phones and PDAs?

A: Depending on the make and model of the device, yes. EnCase Forensic can acquire pictures that are either downloaded or created through the use of the built in camera.

Q. Does information on the device change when I acquire the data?

A: For some devices, it is necessary to place a file on the phone to gain access for acquisitions. To acquire more of the memory, EnCase Forensic has to place a small file in an empty section of the device memory which is removed after the acquisition. This is well documented in the report and does not affect any user data.

Q. Why does the file `DB_notify_register` change when I acquire the device?

A: The file `DB_notify_register` is being constantly changed by the OS. Simply plugging the WinCE device into the charging cradle changes it. Windows CE handles two types of notification events: Timer events and system events. Timer events indicate that a specified time has arrived such as an appointment or a meeting. System events are triggered when the device encounters a change such as AC power connection or disconnection. To support these two types of notification events, the base notification engine maintains two databases: `DB_notify_queue` for timer events and `DB_notify_register` for system events.

CHAPTER 15

WORKING WITH NON-ENGLISH LANGUAGES

Overview 611

Configuring EnCase to Display Non-English Characters 611

Changing the Default Code Page 612

Setting the Date Format 613

Assigning a Unicode Font 613

Viewing Unicode Files 614

Text Styles 615

Configuring Windows for Additional Languages 615

Overview

This chapter describes how to use EnCase when working with evidence in languages other than English.

The Unicode standard attempts to provide a unique encoding number for every character regardless of platform, computer program, or language. Unicode encompasses a number of encodings. In this document, Unicode refers to UTF-16 (Unicode 16-bit Transformation Format). Currently more than 100 Unicode code pages are available. Because EnCase applications support Unicode, investigators can search for and display Unicode characters, and thus support more languages.

EnCase also supports code pages, which describe character encodings for a particular languages or set of languages that use the same superset of characters. In some cases, it is necessary to assign a code page to properly display the language. Thus, EnCase supports both Unicode character sets that do not require a code page as well as legacy character encodings (for example, ISO Latin, Arabic, and Chinese) that do require a specific code page to display properly. You need to use a code page in EnCase only when your non-English document contains a set of these legacy character mappings.

EnCase supports character codes other than 16-bit Unicode for working with non-Unicode, non-English-language text.

Working with non-English languages typically involves performing these tasks:

- Changing the default Code Page. See Changing the Default Code Page on the next page.
- Adjusting the date format. See Setting the Date Format on page 613.
- Assigning a Unicode font. See Assigning a Unicode Font on page 613.
- Creating non-English language search terms.
- Bookmarking non-English language text.
- Viewing Unicode files. See Viewing Unicode Files on page 614.
- Viewing Non-Unicode files.

Configuring EnCase to Display Non-English Characters

When working with non-English languages, an examiner must consider and decide whether to undertake the following tasks.

SETTING THE WINDOWS OPERATING ENVIRONMENT

- If you are running a non-English version of Windows, make sure that you have correctly installed and configured the appropriate Microsoft language pack.
- Make sure that you have installed the set of fonts needed to support the character set for your non-English version of Windows, or have installed a Unicode font.
- Optionally, configure your system to support the keyboard and input language desired.

CONFIGURING ENCASE GLOBAL SETTINGS

- Optionally, set the date format that is commonly used with the language.
- Select a default font for each available user interface element.

USAGE WITH EVIDENCE

- You can create and search for non-English language search terms, bookmark non-English language text, browse through tables and trees in non-English text, etc.
- You can override global settings when viewing content in the **Text** or **Hex** tabs of the View pane. For more information, see Changing Text Styles on page 204.

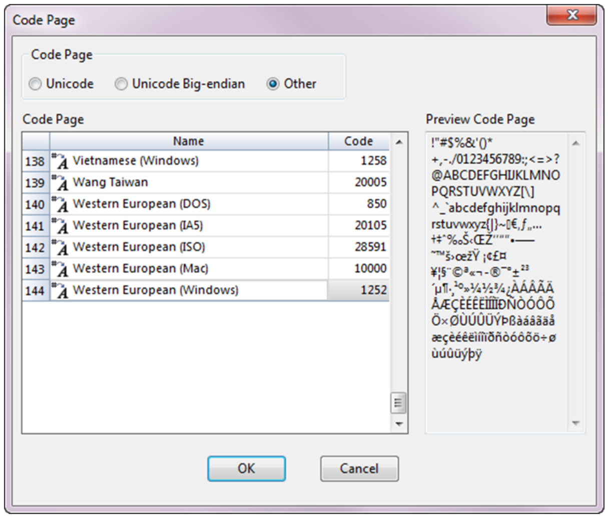
Global internationalization settings are located in the Options dialog. From the **Global** tab you can configure EnCase to display non-English characters in status bars and tabs, dialogs, tables, data views (including text, hex, transcripts), and in the EnScript script editor.

Changing the Default Code Page

The code page you use with EnCase determines the character set required by the language. By default, EnCase uses the default Windows code page (Windows-1252), which handles the majority of Western languages. You can also configure EnCase for Unicode or a specific code page as a global default.

To change the code page:

1. Click **Tools** > **Options**. In the Options dialog select the **Global** tab.
2. Click **Change Code Page**. The Code Page dialog displays.



- **Unicode** specifies little-endian Unicode. If UTF-7 or UTF-8 is used, select **Other**, not Unicode.
- **Unicode Big-endian** specifies big-endian Unicode.
- **Other** lets you select a specific code page from the list.
- Select the appropriate option and click **OK**.

Note: Linux implements special characters (such as German umlauts) using Unicode UTF-8 encodings, but EnCase by default does not decode these 2-byte UTF-8 encodings when it displays the file and folder names. Workaround: Change the Code Page to UTF-8 to see characters with codes above 127. Setting the Code Page in EnCase to UTF-8 if the locale is unknown is better than using the default when an evidence or dd image acquired from *NIX is added to EnCase.

Setting the Date Format

After assigning a code page, you can set the date format to match the selected country:

1. In the Options dialog open the **Date** tab.
2. Configure the desired date and time format. See Date Options on page 39.

Assigning a Unicode Font

If you choose a Unicode option as an EnCase global default, you also must assign a Unicode font for interface elements where non-English language characters display.

1. In the Options dialog, select the **Fonts** tab.
2. Double click the font box for the interface element. The Font dialog opens.

3. Change the font to **Arial Unicode MS** or another available Unicode font and click **OK**.
4. Repeat for each interface element that you want to configure.
5. Click **OK**. The interface elements you selected in the **Fonts** tab are now configured to display characters according to the non-English, Unicode character set. See Font Options on page 42 for more information.

Viewing Unicode Files

Unicode interprets fonts as 16-bit words. When you select Unicode fonts, 8-bit character sets and 7-bit ASCII characters do not display correctly. Use an 8-bit font such as Courier New for English text.

To properly display the characters in certain code pages, you should select a Unicode display font.

Characters that are not supported by the font or code page display as a default character, typically either a dot or a square. Modify this character when using text styles in the **Text** and **Hex** tabs of the View pane.

By default, EnCase displays characters in ANSI (8-bit) format on the **Text** and **Hex** tabs in Courier New font. Viewing Unicode files requires modifications to both the formatting and the font. First, the file or document must be identified as Unicode. This is not always straightforward.

Text files (.txt) containing Unicode usually begin with a Unicode hex signature \xFF\xFE. However, word processor documents written in Unicode are not so easy to identify. Typically, word processor applications have signatures specific to the document, making identification of the file as Unicode more difficult.

You can change the code page from either the **Text** or **Hex** tabs in the View pane by clicking **Codepage**. A list of the most recently used codepages displays.

1. To select a new codepage, click **Codepages**. The Code Pages dialog displays.
2. Select the desired Unicode-based text style. See Changing the Default Code Page on page 612.
3. EnCase updates the text displayed in the **Text** or **Hex** tab to reflect the new encoding.

Text Styles

The display of non-English language content is controlled by both the type face of the content, and the text style applied to the content. A text style applies various font attributes, including:

- Line wrapping
- Line length
- Replacement character
- Reading direction
- Font color
- Class of encoding
- Specific encoding

Text styles are global and can be applied to any case after they are defined. Apply text styles in the **Text** and **Hex** tabs in the View pane. See Changing Text Styles on page 204.

Configuring Windows for Additional Languages

There are several ways you can configure Windows to work with non-English languages. You can configure a keyboard for specific languages. You can also enter non-English content using a character map utility.

Configuring the Keyboard for Additional Languages

Windows lets you configure a keyboard for specific languages. After configuring the keyboard, you must have a keyboard map or familiarity with the keyboard layout of the language.

These instructions are for Windows 7 and Windows 8. Configuring other Windows versions is similar.

To add a keyboard map:

1. Click **Start** and type `change keyboard` in the search bar, or click **Start > Control Panel > Change keyboards or other input methods**. The Keyboards and Languages tab of the Region and Language dialog displays.
2. Click the **Change keyboards** button. The General tab of the Text Services and Input Languages dialog displays.
3. In Installed services, click **Add**. The Add Input Language dialog displays.
4. Click on the plus box next to the language you want to add, click the plus box next to Keyboard, and click the checkbox next to the language you want to add.
5. Click **OK**.

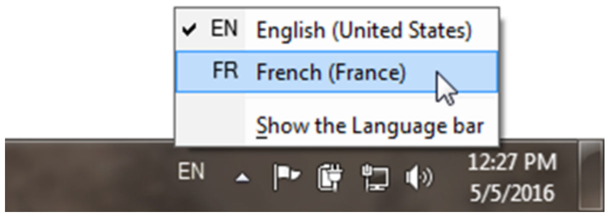
The keyboard is now be mapped to the selected language. Repeat steps 3 and 4 for any additional languages you want to add.

To select and use an installed language map:

1. Click the two letter language code in the notification area of the Windows taskbar.



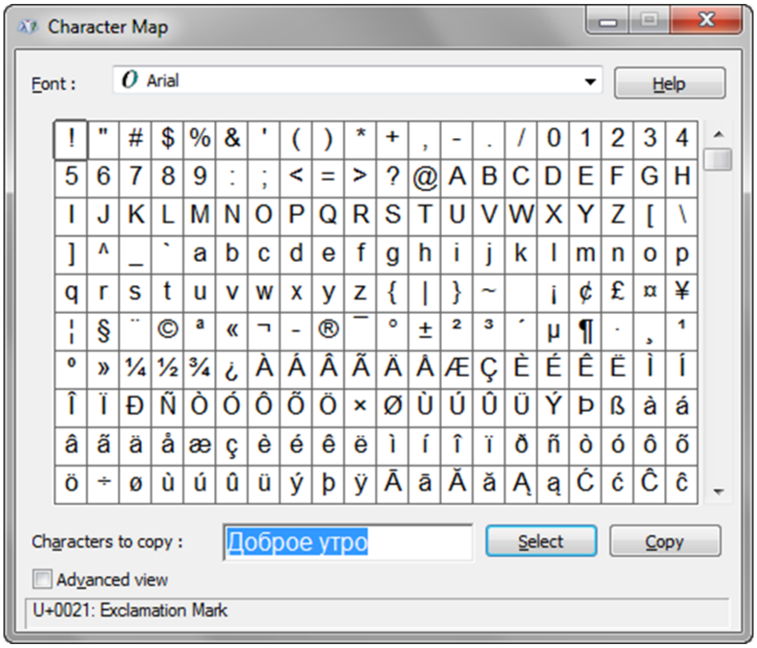
2. Keyboard mapping options display. Select the language you want to use.



Entering Non-English Content with the Windows Character Map

Windows provides a character map utility so you can enter non-English character strings without remapping the keyboard.

1. From the Windows Desktop, click **Start**, type `charmap` into the search box, and press the **Enter** key, or click **Start > All Programs > Accessories > System Tools > Character Map**. The Character Map utility displays.



2. Click the desired character, then click **Select** to add the character to the **Characters to Copy** box.
3. Repeat step 2 to add more characters.
4. Click **Copy**, then paste the characters where you want to use them.

CHAPTER 16

USING LINEN

Overview	621
Creating a LinEn Boot Disk	621
Configuring Your Linux Distribution	622
Performing Acquisitions with LinEn	623
LinEn Manual Page	646

Overview

The LinEn™ utility is an acquisition tool for creating evidence files using a Linux "live" CD/DVD that does not alter any potential evidence on the drives to be acquired. You run the LinEn CD/DVD on a Linux operating system to perform drive-to-drive and crossover acquisitions.

LinEn runs in 32-bit mode, independently of the Linux operating system to quickly acquire data from a large set of devices.

Creating a LinEn Boot Disk

To run LinEn on the subject machine, you must create a LinEn boot disk. Also, you must have an ISO image of one of the popular live Linux distributions you want to use, such as Knoppix, as a Linux distribution does not install itself on the subject machine.

> **Note:** Because it is not practical to modify the settings of a live Linux distribution, ensure that the live distribution does not automatically mount detected devices.

To create a LinEn Boot disk:

1. Using your EnCase application on the investigator's machine, click **Tools > Creat Boot Disk**. The Choose Destination dialog of the Create Boot Disk wizard displays.
2. Click **ISO Image**, then click **Next**. The Formatting Options dialog of the Create Boot Disk wizard displays.
3. Provide a path and filename to the ISO image you downloaded earlier, or click **Alter Boot Table**, and click **Next**. The Copy Files dialog of the Create Boot Disk wizard displays.
4. Right click in the right pane of the Copy Files page, and click **New**. The file browser opens.
5. Enter or select the path to the LinEn executable, usually `c:\program files\encase8\linen`, click **OK**, then click **Finish**. The Creating ISO progress bar displays on the Copy Files dialog. After the modified ISO file is created, the wizard closes.
6. Burn the ISO file onto a blank CD/DVD using the disk burning software of your choice.

You now have a boot disk to run Linux and LinEn while you acquire the subject Linux device.

> **Note:** LinEn does not boot Windows 8 computers when UEFI Mode and Secure Boot are enabled. The new UEFI (Windows 8 BIOS) has additional checks to prevent malicious software from booting Windows 8 computers. Every operating system requires a key. Linux cannot provide this, so it is not allowed to boot. You must disable the UEFI to allow Linux to boot a Windows 8 computer.

Configuring Your Linux Distribution

Before you can run LinEn on Linux, you must configure the Linux distribution. Due to the nature of Linux and its distributions, only the following are discussed:

- SUSE 9.1
- Red Hat
- Knoppix

> **Note:** Because of the dynamic nature of Linux distributions, Guidance Software recommends that you validate your Linux environment before using it in the field.

This process describes an ideal setup that effectively runs the LinEn application in a forensically sound manner.

To prevent inadvertent disk writes, you must make modifications to the operating system. Linux has an **autofs** feature, installed by default, that automatically mounts and writes to any medium attached to the computer. It is essential that you disable **autofs** to prevent automatic mounting.

Obtaining a Linux Distribution

You can obtain a Linux distribution from any Linux vendor.

If you intend to use a LinEn boot disk, you must have a live distribution, such as Knoppix, to create a boot disk. If you intend to run LinEn on an installed version of Linux on your examiner machine, we recommend SUSE or Red Hat.

For the Linux distributions discussed in relation to LinEn, obtain a distribution from one of the following:

- For the latest SUSE distribution, go to the Suse website (http://www.suse.com).
- For the latest Red Hat distribution, go to the Red Hat website (http://www.redhat.com).
- For the latest Knoppix distribution, go to the Knoppix website (http://www.knoppix.org).

LinEn Setup Under SUSE

To perform this setup process, you must have SUSE installed on your Linux machine.

1. Copy the LinEn executable from `C:\Program Files\EnCase8` on your Windows machine to the desired directory, `/usr/local/encase` on your Linux machine.
2. Open a command shell on your Linux machine and run LinEn as root/super user.
3. Enter `chmod 700 /usr/local/encase/linen`. This changes the permissions on the LinEn executable, so that it can only be executed by root/super user.
4. Close the command shell.
5. Click **Main Menu > System > Configuration > YaST**. Yet Another Setup Tool (**YaST**) is used to configure various settings for your Linux operating system.
6. Open the Runlevel Editor.
7. Ensure that **autofs** is disabled.

LinEn Setup Under Red Hat

To perform this setup process, you must have Red Hat installed on your Linux machine.

1. Copy the LinEn executable from `C:\Program Files\EnCase8` on your Windows machine to the desired directory, `/usr/local/encase` on your Linux machine.
2. Open a command shell on your Linux machine and run LinEn as root/super user.
3. Enter `chmod 700 /usr/local/encase/linen`. This changes the permissions on the LinEn executable, so that it can only be executed by root/super user.
4. Close the command shell.
5. Click **Main Menu > System Settings > Server Settings**.
6. Ensure that **autofs** is disabled.

Performing Acquisitions with LinEn

The EnCase LinEn utility provides the following methods of acquiring evidence from a subject drive:

- Drive-to-drive acquisitions
- Crossover cable acquisitions

Drive-to-drive acquisitions provide the means to safely preview and acquire devices without using a hardware write blocker. Drive-to-drive acquisitions use either the subject machine or the forensic machine to perform the acquisitions.

Crossover cable acquisitions require both a subject and forensic machine. This type of acquisition also does not require a hardware write blocker. It may be desirable in situations where physical access to the subject machine's internal media is difficult or not practical. This is the recommended method for acquiring laptops and exotic RAID arrays. This method is slower than a drive-to-drive acquisition because data is transferred over a network cable, making it especially sensitive to the speed of the network cards housed in both machines.

Setup for a Drive-to-Drive Acquisition

When a subject drive from the subject machine cannot be acquired via a crossover cable acquisition, the subject drive can be acquired via a drive-to-drive acquisition. Drive-to-drive acquisitions can be done in the following ways:

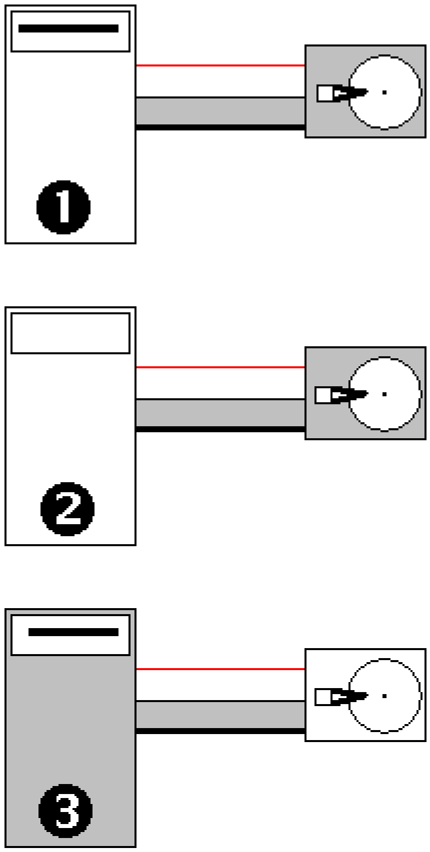
- Running a LinEn boot disk on the forensic machine
- Running the LinEn utility from Linux already installed on the forensic machine
- Running a LinEn boot disk on the subject machine

Any of these cables can be used as a hard disk cable:

- IDE Cable
- USB Cable
- Firewire
- SATA
- SCSI

The following diagrams show setups for drive-to-drive acquisitions:

1. The forensic machine, running LinEn from the LinEn Boot Disk, connected to the subject hard drive.
2. The forensic machine, booted to Linux and running LinEn, connected to the subject hard drive.
3. The subject machine, running LinEn from the LinEn Boot Disk , connected to the target hard drive.



Drive-to-Drive Acquisition

Before you begin, identify the subject drive to be acquired and the storage drive to hold the acquired evidence file.

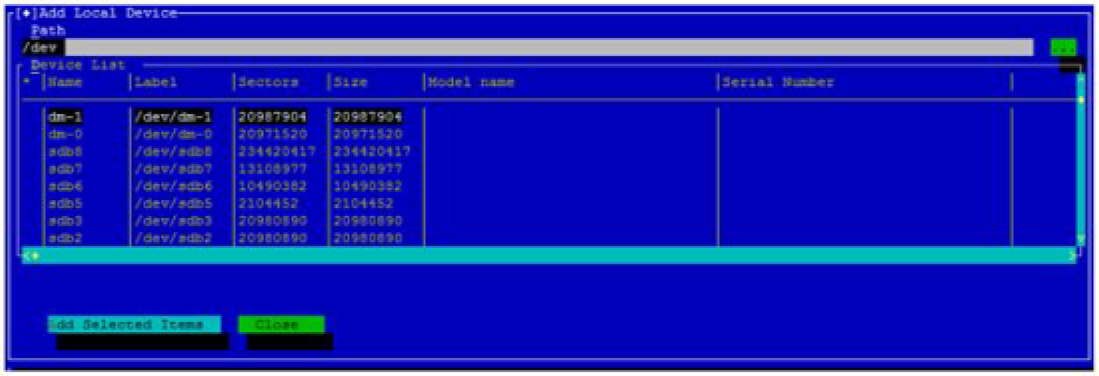
If the FAT32 storage partition to be acquired has not yet been mounted, do so.

Navigate to the folder where LinEn resides and enter `./linen` in the console. The LinEn main window displays.

Load Local Device

To acquire a device, you first load a local device.

1. Select the **Load** menu > **Local Devices** option to add a local device to the Device Window.
2. The Add Local Device dialog displays. Here you can add one or more devices to LinEn.



The Add Local Device dialog contains a list of all devices, both full drives and partitions.

PATH

The **Path** option changes the directory scanned for devices. Selecting **Path** and pressing **Enter** opens a dialog that changes the directory according to your input.

DEVICE LIST

For each device, the following information is displayed:

- **<checkbox>**: Checked when the device is selected.
- **Name**: Filename of the block device as it is seen in the /dev directory. This is the same name displayed in EnCase.
- **Label**: Full path to the device.
- **Sectors**: Number of sectors for this device.
- **Size**: Size of the device in bytes.
- **Model name**: Model name reported by the operating system. Logical devices don't have model names.
- **Serial Number**: Serial number reported by the operating system. Logical devices don't have serial numbers.

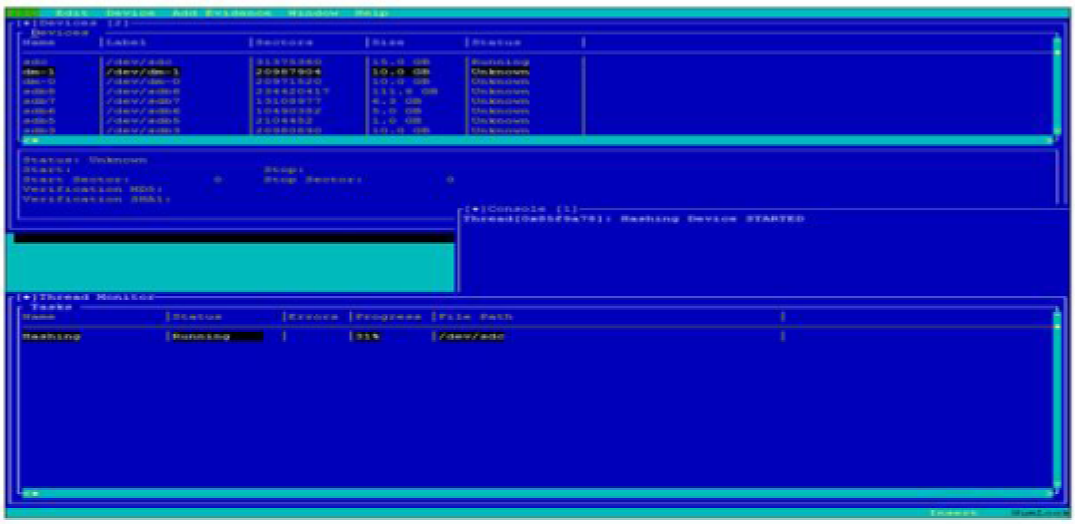
The columns displayed in the Add Local Device window can be scrolled using the scroll bar at the bottom or the left and right arrow keys.

One device is currently highlighted with a black background. Pressing the arrow keys moves the highlighted selection. Pressing the PageUp and PageDown keys moves the highlighted selection by one page. Pressing the Space key selects a device. Choose **Select All** from the **Edit** menu, or press **Ctrl+A** to select all devices.

After selecting one or more devices, select **Close to** add the devices to LinEn. No processing of the devices, such as hashing, is done at this time.

Devices Window

At startup, the Devices window is empty. It is populated when you add devices. After being populated, the Device Window displays.



The Devices Window contains the following information for each device that has been added.

- **Name**: Filename of the block device as it is seen in the /dev directory. The same name displays in EnCase.
- **Label**: Full path to the device.
- **Sectors**: Number of sectors for this device.
- **Size**: Size of the device in bytes.
- **Status**: Indicates if the device has been hashed or acquired. Values for this field are Unknown, Running, Done, and Cancelled.

When a device is selected, its text displays on a black background. Selected devices can be hashed, acquired, added, deleted or saved.

Adding and Removing Devices

To add devices to the Devices Window, select **Load > Local Devices**.

To remove the selected device, use the **Delete** option either from the menu, or by pressing the **Delete** key. Note that this removes the device from LinEn only. No changes such as deleting files or formatting are made to the actual device.

Acquiring a Device

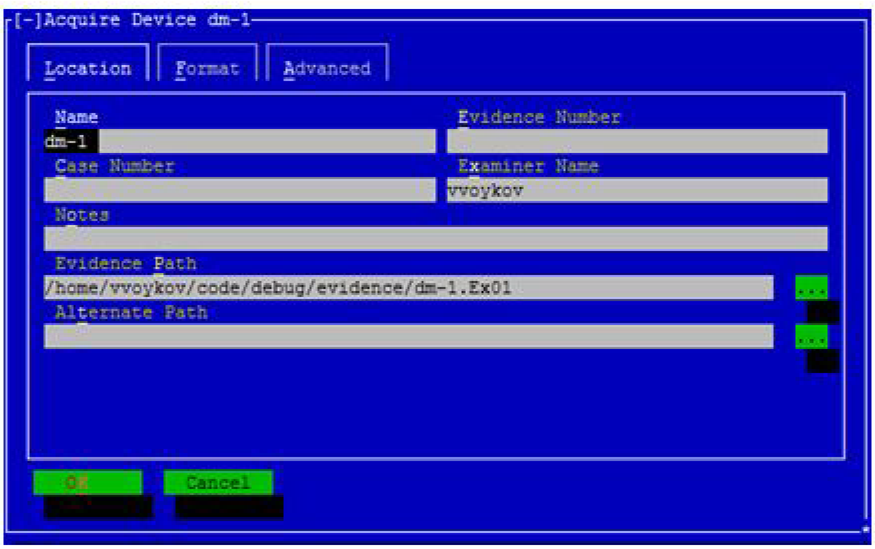
The **Acquire** menu option begins acquisition of the currently highlighted device. As acquisition begins, the Acquire Device dialog displays, with the following three tabs:

- **Location**
- **Format**
- **Advanced**

After you set the parameters in the Acquire Device dialog and click **OK**, acquisition begins. A thread is added to the Thread Monitor.

ACQUIRE DEVICE DIALOG LOCATION TAB

The Acquire Device dialog **Location** tab sets file location information used when acquiring a device.



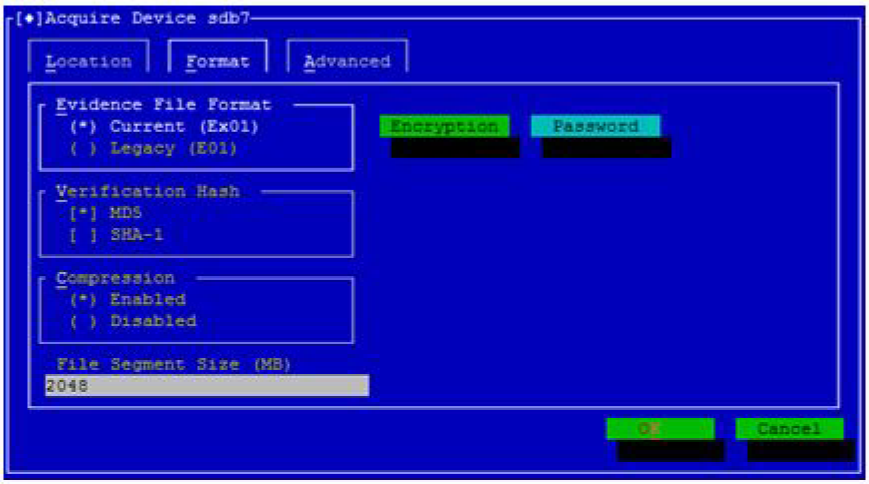
The Acquire Device dialog **Location** tab displays the following fields and options.

- **Name**: Generates the name of the file in the Output Path control. By default, the Name field has the same value as the name in the Devices Table in the Device Window. Changing this value changes the name of the file.
- **Evidence Number**: Stored in the evidence file as Evidence Number.
- **Case Number**: Stored in the evidence file as Case Number.
- **Examiner Name**: Stored in the evidence file as Examiner Name.
- **Notes**: Free text up to 32 characters. Stored in the evidence file.
- **Output Path**: Evidence File Path. Use to enter or browse to a different output path.

- **Alternate Path**: A semicolon delimited list of alternate paths, used to enter or browse to an alternate path. The alternate path provides a secondary location for LinEn to use for continuing to write segments of the evidence file if the location designated by the Output Path does not have enough space to write the entire evidence file.

ACQUIRE DEVICE DIALOG FORMAT TAB

The Acquire Device dialog **Format** tab sets format options used when acquiring a device.



The Acquire Device dialog **Format** tab displays the following fields and options.

Evidence File Format: Specifies the evidence file format. The default evidence file extension is Ex01. A legacy evidence file (a file using the format in versions of EnCase prior to Version 8) is E01. Note that selecting **Legacy** enables the **Password**button. Using a password in EnCase legacy evidence files is optional. To use one, click **Password** to open a dialog to enter and confirm a password. Keep a record of the password in a secure location. EnCase does not have a password recovery tool.

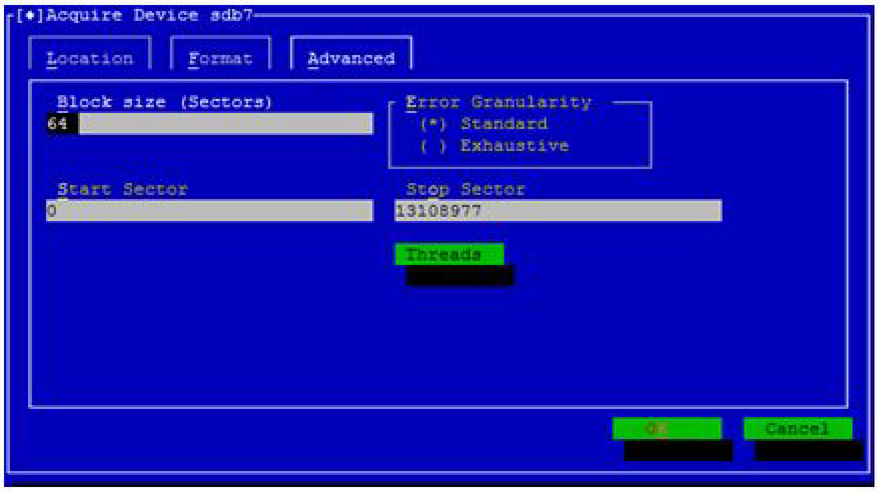
- **Verification Hash**: Dropdown list for hashing algorithms includes the following selections:
  - **None**: No check boxes are selected.
  - **MD5:** Selects MD5.
  - **SHA-1:** Selects SHA-1.
  - **MD5 and SHA-1**: Both check boxes are selected.

- **Compression**: Specifies whether compression is enabled.
- **File Segment Size**: Specifies the file segment size (MB) (minimum: 30MB, maximum: 8,796,093,018,112MB, default: 2048MB).
- **Encryption** button: Opens the Encryption Details dialog. This is enabled for Ex01 evidence files only.

- **Password** button: Opens the Password dialog. This is enabled for E01 (legacy) evidence files only.

ACQUIRE DEVICE DIALOG ADVANCED TAB

The Acquire Device dialog **Advanced** tab sets block size and sector options used when acquiring a device.

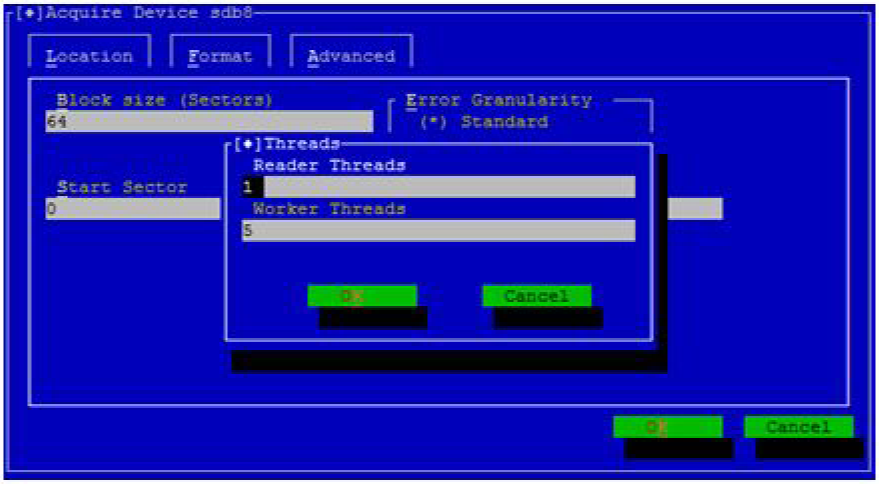


The Acquire Device dialog **Advanced** tab displays the following fields and options.

Block Size (Sectors): (Minimum: 64, maximum: 1024). Higher block sizes allow slightly faster acquisitions and create smaller evidence files. However, with large block sizes, when evidence files are damaged, larger blocks of data are lost.

- **Error Granularity**: Portion of the block zeroed out if an error is encountered.
  - **Standard**: Same value as the block size.
  - **Exhaustive**: Sets granularity to one sector. This retains more data but takes more time.

- **Start Sector**: Specifies the start sector (minimum: 0, maximum: maximum number of sectors of the source).
- **Stop Sector**: Specifies the stop sector (minimum: 0, maximum: maximum number of sectors of the source).
- **Threads**button: Displays the Threads dialog.



- ◦ **Reader Threads**: Controls how many threads are reading from the source device, enabled only if the file format is E01. (1-5 available; default is 0).
- ◦ **Worker Threads**: Controls data compression calculation, enabled for both EnCase evidence file formats, E01 and Ex01. (1-20 available; default is 5).

The Device Window

The results of acquiring a device display in the Device Window.

If the device has not been acquired, the Name, Start Sector, and Stop Sector are populated and all other fields are blank.

After acquiring begins, the Start time displays. When you select a device, if the device has been acquired, the following information displays:

- **Status**: Acquiring (while the thread is running). Acquired (when the operation finishes).
- **Start**: Start time of the operation.
- **Stop**: Finish time of the operation.
- **Time**: Elapsed time of the operation.
- **Start Sector**: Start sector of the part of the device that is hashed. By default, if you hash the full device, this value is 0.
- **Stop Sector**: Final sector of the part of the device that's hashed. By default (if you hash the full device), this is the maximum sector number.
- **Verification MD5**: MD5 hash of the part of the device that is hashed. This displays only when you select MD5 in hash options.
- **Verification SHA1**: SHA1 hash of the part of the device that is hashed. This displays only when you select SHA1 in hash options.

If you acquire a device more than once, the display is cleared of old information, and displays only new information.

If you try to hash a device that is currently being used in LinEn (for example, already hashing or acquiring), a dialog asks if the current thread should be canceled. A new hashing thread for the same device is created only when the current thread is not running.

Saving Acquisition Information

After acquiring one or more devices, you can save the acquisition information to a file. You can select this option from the menu (or with the Ctrl-S keyboard command) if the current top window is the Device Window and the selected device is hashed. The information displayed in the status pane is saved in a file.

The file name is automatically generated and cannot be changed. For example, acquisition information for a device with the name "hdd1" is saved in: `[current directory]/hdd1.acq`. If the file already exists, the new information is appended to the end of the file.

LinEn Evidence Verification

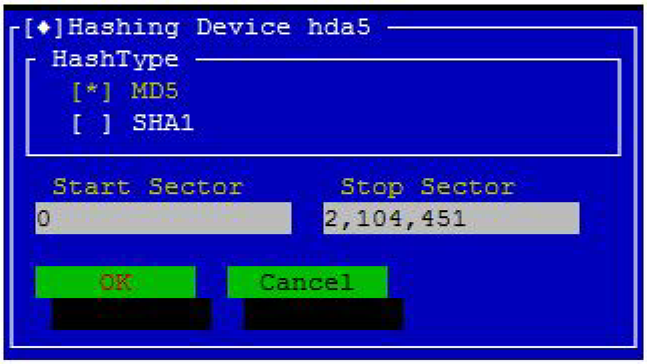
After acquiring a device, you can verify that the evidence file is correct in two ways:

1. Verify individual segments of the evidence file (for example, the .EO3 segment). This confirms that the files are not corrupted, but does not confirm that the files match the underlying device.
2. Hash the original device and the acquired evidence image, then compare the hashes to make sure that the correct data has been acquired.

Hashing a Device

To hash a device, first load a device, as described in the Load Local Device section. Once loaded, follow this process to perform a hash.

The **Device/Hash** option hashes a device or part of a device, using MD5, SHA1, or both. This option opens the Hashing Device dialog.



Use this dialog to select the type of hash: **MD5** or **SHA1**. You can also select both or no option. The hash type options are checkboxes. You can select or clear them independently using the **Space** bar.

Use this dialog to select start and stop sectors. When you open this dialog, the Start Sector and Stop Sector fields are populated with 0 (Start Sector) and the maximum sector (Stop Sector).

Clicking **OK** starts the hashing process, changes the status of the device in the Devices Window, and creates a new thread in the Thread Monitor Window. Both hash values are calculated in the same thread, so only one thread is started. If none of the check boxes is selected, the dialog exits and no thread is created.

After completion, hash information is displayed in the Device Window. You can save this information to a file.

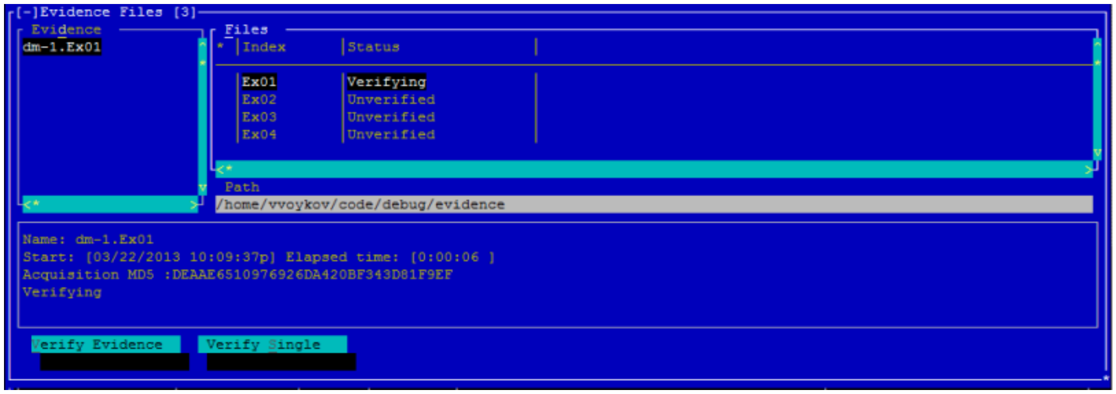
SAVING DEVICE HASHING INFORMATION

After a device has been hashed, it can be saved when selected in the Device Window. The information displayed in the status pane is saved in a file.

The filename is generated automatically and cannot be changed. For example, a device with the name hdd1 is saved in: `[current directory]/hdd1.hash`. If the file already exists, the new information is appended to the end of the file.

Verifying Evidence Files

To verify an evidence file, load the evidence file from the Evidence Files Window.



The Evidence Files window contains information about the evidence displayed in the Evidence box on the left and the segments they contain if the evidence has multiple files, shown in the Files box on the right.

Changing the current selection in the Evidence list will refresh the list of the files.

The **Verify Evidence** button uses the current selection from the Evidence box to begin verifying the entire evidence. If the evidence file does not have acquisition information, the verification begins and verifies the evidence to ensure that the file is readable. In this example, the verification is done after selecting all segments and clicking the Verify Single button. No hash value is calculated.

The **Verify Single** button uses the current selection from the Files box and verifies the selected evidence segments. The Single file verification only option reads a segment to make sure that it is readable and that the information is consistent.

Information about the selected evidence is shown below.

- If the evidence has not been verified, the Name, Acquisition, MD5, and SHA1 fields and are populated. The other fields are blank.
- Once verification begins, the start time is shown.
- If the evidence has been verified, verification information for MD5 and SHA1 displays.

This information contains:

- **Name**: Name of the evidence.
- **Start**: Start time of the verification operation.
- **Elapsed Time**: Elapsed time of the verification operation.

The following fields are optional. Their values depend on the results of the verification.

- **Acquisition MD5**: The MD5 hash of the evidence file when created. Not displayed if MD5 is not selected during the acquisition.
- **Acquisition SHA1**: The SHA1 hash of the evidence file when created. Not displayed if SHA1 is not selected during the acquisition.
- **Verification status**: Status of the verification.
- **Verification MD5**: Displays only if it does not match the Acquisition MD5 value after the verification ends.
- **Verification SHA1**: Displays only if it does not match the Acquisition SHA1 value after the verification ends.

ACQUISITION MD5

- Before the verification, this is the MD5 hash of the evidence file when it was created.
- After the verification ends:
  - If no errors occur, this value is replaced with the MD5 hash value.
  - If the verification fails, this value remains and the verification MD5 displays.

ACQUISITION SHA1

- Before the verification, this is the SHA1 hash of the evidence file when it was created.
- After the verification ends:
  - If no errors occur, this value is replaced with the SHA1 hash value.
  - If the verification fails, this value remains and the verification SHA1 displays.

VERIFICATION STATUS

- **Unverified**: Displays before evidence file verification begins.
- **Verifying**: Displays during the verification.
- **Verified**: Displays after the verification thread finishes. Status values include:
  - **Verified, no errors**: Indicates the verification process did not find any errors.
  - **Verify errors #**: Displays the number of errors found during the verification process.

If the verification is started again, the display is cleared, and displays new information.

If a verification is already in progress (the thread status displays as Running) and you attempt to verify the same evidence, a dialog displays giving you the option to cancel the current thread. A new verification thread for the same device is created only when the current thread is not running.

To add evidence files to the Evidence Files window, use the Add Evidence menu.

To remove the selected evidence, use the **Delete** option from the menu, or press the **Delete** key.

The **Save** command saves the information to a file using the same name as the evidence file.

SAVING EVIDENCE VERIFICATION INFORMATION

To save evidence verification information, select the **Save** option from the Device Window (or enter Ctrl-S). The information displayed in the status pane is saved in a file.

The filename is automatically generated and cannot be changed. For example, a device with name" hdd1" is saved in: `[current directory]/hdd1.verify`. If the file already exists, the new information is appended to the end of the file.

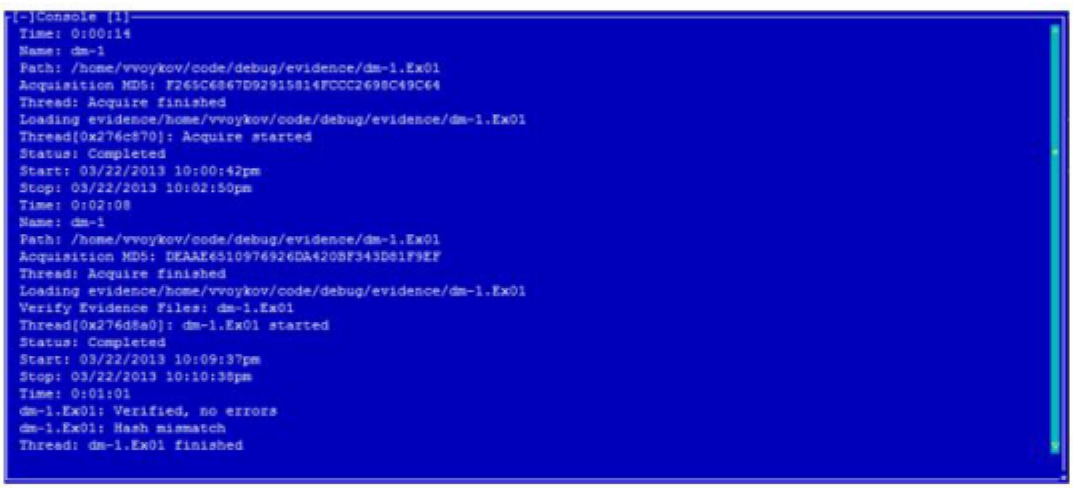
Window Menu

The Window Menu is the starting navigation point for using LinEn. This window has five options.

- **Refresh**: Redraws the whole screen.
- **Console**: Opens the Console window.
- **Thread Manager**: Opens the Thread Monitor window.
- **Devices**: Opens the Device window.
- **Evidence**: Opens the Evidence window.

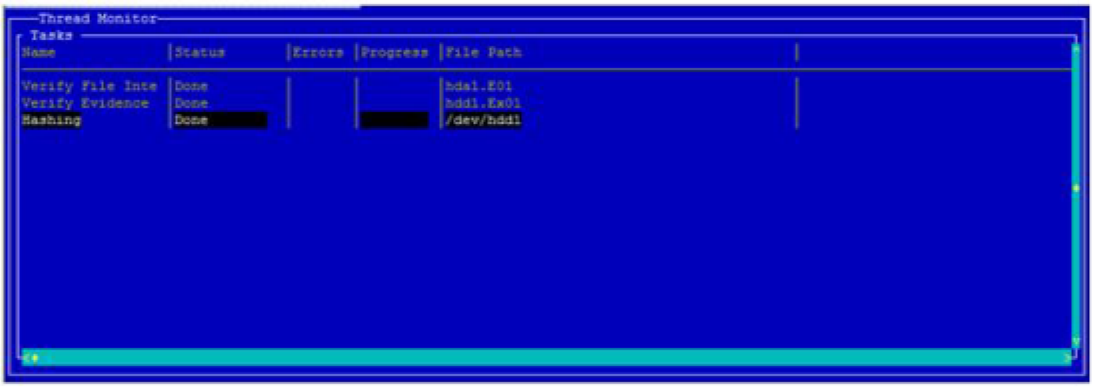
Console Window

The LinEn Console Window has the same function as the EnCase console. All error or information messages display in this window. For example, when a verification or acquisition finishes, the result displays in the Console window.



Thread Monitor Window

The Thread Monitor window contains information about threads (tasks) that are running or have run, including current status and progress percentage.



LinEn creates threads when the following tasks are initiated:

- Hashing
- Single file verification
- Evidence file verification
- Evidence acquisition

For each thread, the following information displays:

- **Name**: Name of the type of thread, such as hashing device, verify single, verify evidence, acquire.
- **Status**: Thread status, such as running, suspended, canceled, done.
- **Errors**: The number of errors. This is blank if there are no errors.
- **Progress**: Percent completion, 100% = completed.
- **File Path**: A processing comment. For example, "Hashing: /dev/hda5" or "Verifying: myfile.E01".

If you select a thread and press the **Delete** key:

- If the thread is running, LinEn:
  - Displays a confirmation box.
  - Displays a dialog with the option to cancel the thread.
  - Removes the thread from the Thread Monitor list.
- If the thread is not running, LinEn:
  - Removes the thread from the Thread Monitor list.

Threads are shown until removed by deletion. The status window shows a history of actions performed.

ENDING A JOB OR TASK

If you begin running a job or task, such as hashing, acquiring, or verifying evidence, and need to end it before it finishes, press the **Delete** key while in this window.

Edit Menu

The top level window in Linen includes an **Edit** menu option. The Edit menu contains **Delete** and **Options** selections, described below.

DELETE

Content deleted is context-dependent.

- If the current top window is the Device Window, the currently selected device is deleted from the table. It is removed from LinEn, not deleted on disk. When a device is deleted it is removed from the LinEn Devices Window.
- If the current top window is the Evidence Files Window, the currently selected evidence is deleted.
- If the current top window is the Thread Monitor Window, the currently selected thread is deleted. If the thread is currently running, LinEn asks if you want to cancel it.

If a running thread is associated with the current item you want to delete, LinEn will ask if you want to cancel the thread before the item is removed from the table.

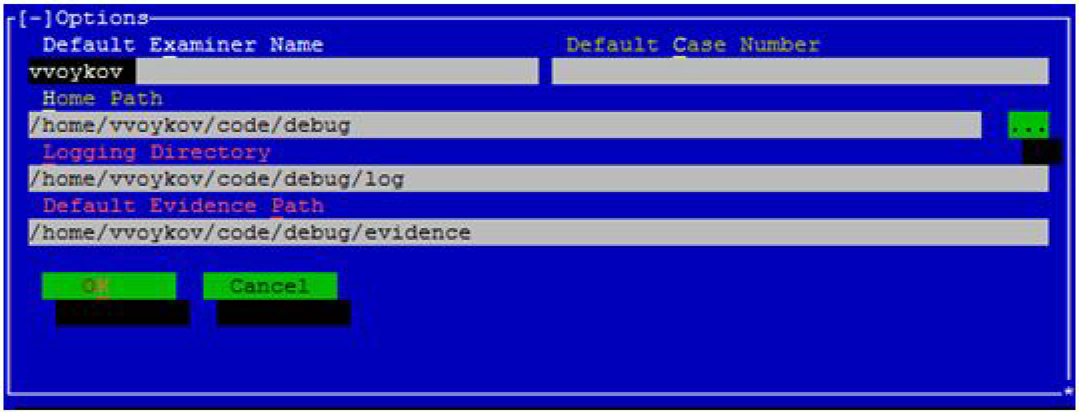
- If you select **No**, the thread is resumed and the item is not deleted.
- If you select **Yes**, the thread is cancelled and the item is deleted.

> **Note:** The thread itself is not deleted from the Task Manager window, unless this is the current window.

> **Note:** When anything is deleted from current window, LinEn does not give you the option to save textual data, such as hash results.

OPTIONS

The Options window sets commonly used variables.



DEFAULT EXAMINER NAME

By default the Default Examiner Name field is set to the username of the account that is running LinEn. If the value is set, the text is transferred to the Examiner field in the Acquisition dialog.

DEFAULT CASE NUMBER

Default Case Number works in the same way as examiner name, but the value is transferred to the Case Number field in the Acquire dialog.

HOME PATH

The Home Path field points to a directory. If the directory path does not exist, LinEn creates it when you click **OK**. This directory is used as a root directory to organize stored information, such as logs and evidence files.

LOGGING DIRECTORY

Logging Directory is a read-only field. It cannot be edited. It displays where the logs are stored when saving information fields or the console.

DEFAULT EVIDENCE PATH

Default Evidence Path is similar to the Logging Directory, but shows where by default the evidence files are stored.

Both the Logging Directory and Default Evidence Path fields contain recommended values. The values in these fields are transferred to the corresponding fields in the Acquire dialog. You can change the fields in the Acquire dialog.

LinEn Command Line

You can run LinEn from a command line to execute most of the functions described in prior sections of this chapter.

Note: You must use the `-cl` option to activate this feature.

Select an operation:

- `-k` for AcquireMode
- `-o` for HashMode

Note: You must choose either AcquireMode or HashMode. LinEn displays an error message if you attempt to use both.

You can enter command line options with a single dash and the shortcut (for example, `-p <Evidence Path>`) or with a double dash and the full tag (for example, `--EvidencePath <EvidencePath>`).

During the acquisition or hashing process, a pipe character (|) prints to the console for each percentage completed.

The two ways to provide necessary information to LinEn include:

- Command line options
- Configuration file

COMMAND LINE OPTIONS

Shortcut	Full Tag	Description
-dev <Device Path>	Device	Device to be either acquired or hashed.
-p <Evidence Path>	EvidencePath	Path and filename of the evidence to be created (maximum 32,768 characters).

Shortcut	Full Tag	Description
-m <Evidence Name>	EvidenceName	Name of evidence within the evidence file (maximum 50 characters).
-c <Case Number>	CaseNumber	Case number of the evidence (maximum 64 characters).
-x <Examiner>	Examiner	Examiner's name (maximum 64 characters).
-r <Evidence Number>	EvidenceNumber	Evidence number (maximum 64 characters).
-a <Alternate Paths>	AlternatePath	A semicolon delimited list of alternate paths (maximum 32,768 characters).
-n <Notes>	Notes	Notes (maximum 32,768 characters). Enclose notes in quotes (for example, "This is a note").
-l <Max File Size>	MaxFileSize	Maximum file size of each evidence file (in MB: minimum 1, maximum 10,485,760).
-d <Compress>	Compress	Level of compression (0=none, 1=fast, 2=best).
-g <Granularity>	Granularity	Error granularity in sectors (minimum 1, maximum 1024).

Shortcut	Full Tag	Description
-b <Block Size>	BlockSize	Sectors per block for the evidence file (minimum 1, maximum 1024).
-ev2	EV2	Evidence file format V2.
-f <Configuration File>	File	Path to a configuration file holding variables for the program (maximum 32,768 characters).
-t	Hash	Perform MD5 hashing on device.
-1	SHA1	Perform SHA-1 hashing on device.
-cl	CommandLine	Do not ask for required values, just error out.
-k	AcquireMode	Acquire the selected device.
-o	HashMode	Hash the selected device.
-?		Help message.
-pw <password>		Password protects the resulting evidence file. The -pw option is not supported for *.Ex01 evidence files.

Shortcut	Full Tag	Description
-date <date/time>		Lets the user enter the correct date/time. Must be quoted in the format "MM/dd/yy hh:mm:sstt" or "MM/dd/yy hh:mmtt" (where tt is AM or PM).
-rdr <number>	Readers	Number of reader threads (acceptable value 1-5).
-wrk <number>	Workers	Number of worker threads (acceptable value 1-20).
-hsh	Hasher	Hash in its own thread (default: false).
-rerr	ReadErrors	Print read errors to STDERR (default: false).
-v	Verbose	Verbose output during acquisition or hashing (default: false) (acceptable value TRUE or FALSE [only in file]).

NON INTERACTIVE COMMAND

- If (`-cl)` is set, LinEn is non interactive, allowing third party software to use its own scripting.
- If (`-cl`) is set, users must pass all LinEn settings via a text file or via command line arguments.

CONFIGURATION FILE

You can create a configuration file to fill in some or all of the variables. The configuration file must be in the format OptionName=Value. All of these options have the same restrictions as their command line counterparts.

Options for the configuration file include:

EvidencePath	Path and filename of the evidence to be created
EvidenceName	Name of the evidence within the evidence file
CaseNumber	Case number of the evidence
Examiner	Examiner's name
EvidenceNumber	Evidence number
AlternatePath	A semicolon delimited list of alternate paths
Notes	Optional notes
MaxfileSize	Maximum file size of each evidence file
Compress	Level of compression (0=none, 1=fast, 2=best)
Granularity	Error granularity in sectors
BlockSize	Sectors per block for the evidence file
Hash	Turn on (TRUE) or turn off (FALSE) MD5 hashing
SHA1	Turn on (TRUE) or turn off (FALSE) SHA-1 hashing
Device	Device to be acquired or hashed
CommandLine	Exit if a required variable is not filled out (TRUE or FALSE)
AcquireMode	Acquire the device chosen (TRUE or FALSE)
HashMode	Hash the device chosen (TRUE or FALSE)
EV2	Evidence file format V2

Note: Any options specified on the command line take precedence over those in the configuration file.

Once the selected operation is complete, results print to the console. Read errors and read error sectors display only if there are actual errors.

HASHING RESULTS

Name: <EvidenceName>

Sectors: 0-<TotalSectors>

MD5 Value: <Md5Value>

SHA1 Value: <SHA1Value>

Read Errors: <ReadErrors> The hash value may not be accurate

Read Error Sectors: <start1>-<stop1>, <start2>-<stop2>, etc.

ACQUISITION RESULTS

<EvidenceName>: acquired to <EvidencePath>

Elapsed Time: <ElapsedTime>

MD5 Value: <Md5Value>

SHA1 Value: <SHA1Value>

Read Error Sectors: <start1>-<stop1>, <start2>-<stop2>, etc.

Crossover Cable Preview or Acquisition

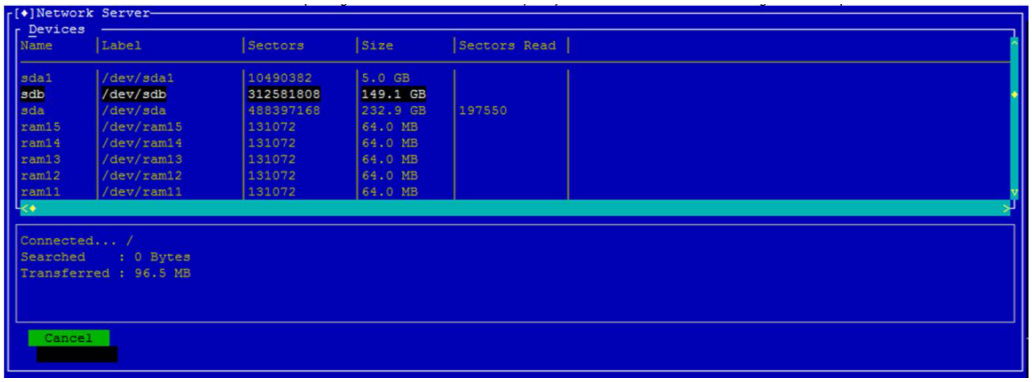
To perform a crossover cable preview or acquisition, you must have access to a LinEn boot disk or another LinEn bootable device. The investigator must have identified the subject drive to acquire.

To do a crossover cable preview or acquisition:

1. Boot the target machine from the LinEn bootable device. Ensure the target machine has an operable optical drive or USB port and can actually boot from a CD or bootable LinEn device.
2. Connect the forensic machine to the subject machine using a crossover cable or an Ethernet cable.

   Note: If an Ethernet cable is used, both the target and forensic machine must have gigabit Ethernet.

3. On the target machine running LinEn, ensure an IP address has been assigned correctly to the default Ethernet adapter by typing `ifconfig eth0`. If the adapter does not have an IP address assigned, assign one manually by typing `ifconfig eth0 10.0.0.2 netmask 255.0.0.0`. Verify the IP address assignment completed successfully by typing `ifconfig eth0`.
4. Navigate to the folder where LinEn resides and type `./linen` in the console to run LinEn in Server Mode.
5. When you select a device, a variation of the following information displays:



6. On the forensic machine, modify the network adapter settings in Windows to place the machines in the same network, IP address of 10.0.0.3 and subnet mask 2555.0.0.0. You should be able to ping the target machine running LinEn at this point.
7. Launch EnCase on the forensic machine.
8. On the Home page, create a new case or open an existing case.
9. Click **Add Evidence** > **Add Crossover Preview**. The Add Crossover window displays, and lists crossover devices.
10. Select **Network Crossover**, and click **Select**.
11. Select the physical disk or logical partition to acquire or preview and click **OK**.

You can preview and acquire the contents of the device through EnCase. For more information about acquisition, see Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA) on page 107 and Acquiring a Disk Running in Direct ATA Mode on page 109.

LinEn Manual Page

LinEn includes a man page containing detailed information on block size and error granularity. You can access it via the command line or from the **Help** button in the user interface.

ACCESSING FROM A COMMAND LINE

1. Place the `linen.1.gz` file in one of the man paths.
2. Type the command `man linen`.
3. Press **Enter**.
4. The man page displays.

```
File  Edit  View  Terminal  Tabs  Help
linen(1)                                                        linen(1)

NAME
       linen - Acquire EnCase evidence files

SYNOPSIS
       linen     -cl    -k    -dev devicepath -p evidencepath -m evidence-
       name -c casenumber -x examiner -r evidencenumber -d compress
       [-a alternatepaths]  [-n notes]  [-l maxfilesize]  [-g granularity]
       [-b blockSize]    [-j file]     [-date datetime]     [-pw password]
       [-wrk workers]  [-rdr readers] [-t] [-1] [-hsh] [-verify] [-e] [-v]
       [-rerr]

       linen -cl -o -dev devicepath [-t] [-1]

       linen -cl -verify -p evidencepath

       linen -s

       linen -?

DESCRIPTION
        Linen allows the acquisition of devices to EnCase evidence  files,
       computation  of  MD5 and/or SHA1 hashes for devices or verification
       of evidence files.

OPTIONS
:
```

CHAPTER 17

ENCASE DECRYPTION SUITE

Overview	652
Disk and Volume Encryption	652
Supported Encryption Products	653
EDS Commands and Tabs	655
Safeboot Encryption Support	660
Check Point Full Disk Encryption Support (Volume Encryption)	663
BitLocker Encryption Support (Volume Encryption)	667
WinMagic SecureDoc Encryption Support	675
WinMagic SecureDoc Self Encrypting Drive (SED) Support	677
GuardianEdge Encryption Support	678
Symantec Endpoint Encryption Support	681
Sophos SafeGuard Support	682
Utimaco SafeGuard Easy Encryption Support	685
PGP Whole Disk Encryption (WDE) Support	689
Dell Data Protection Enterprise (formerly Credant Mobile Guardian) Encryption Support	691
McAfee Endpoint Encryption Support	694
S/MIME Encryption Support	695
NSF Encryption Support	696
Lotus Notes Local Encryption Support	697
Windows Rights Management Services (RMS) Support	700

Windows Key Architecture 701
Dictionary Attacks 702
Built-In Attacks 703

Overview

EnCase Decryption Suite (EDS) enables the decryption of encrypted files and folders by domain and local users. EDS is included with EnCase Forensic in most countries. EDS supports the following forms of encryption:

- Disk and volume encryption
    - Microsoft BitLocker
    - GuardianEdge Encryption Plus/Encryption Anywhere/Hard Disk Encryption
    - Utimaco SafeGuard Easy
    - McAfee SafeBoot
    - WinMagic SecureDoc Full Disk Encryption
    - PGP Whole Disk Encryption
    - Checkpoint FDE (Full Disk Encryption)

- File based encryption
    - Microsoft Encrypting File System (EFS)
    - Credant Mobile Guardian
    - Dell Data Protection
    - RMS

- Mounted files
    - PST (Microsoft Outlook)
    - S/MIME encrypted email in PST files
    - NSF (Lotus Notes)
    - Protected storage (ntuser.dat)
    - Security hive
    - Active Directory 2003 (ntds.dit)
    - EnCase Logical Evidence File Version 2 Encryption

Disk and Volume Encryption

When an evidence file (.E01) or a new physical disk is added to a new case, EnCase Forensic checks the Master Boot Record (MBR) against known signatures to determine whether the respective disk is encrypted.

If the disk is encrypted, EnCase Forensic requests user credentials (see Supported Encryption Products below for a table listing required credentials for supported encryption products). Note that the disk/volume encryption support in EnCase Forensic works only at the physical level.

- If the credentials are not correct, the User Credential dialog displays again. If this occurs, enter the correct credentials to exit the dialog or press **Cancel**.
- If the correct credentials are entered, EnCase Forensic decrypts the disk. No password attacks are supported.

EDS supports these disk/volume encryption products:

- Microsoft BitLocker
- GuardianEdge Encryption Plus/Encryption Anywhere/Hard Disk Encryption
- Utimaco SafeGuard Easy
- McAfee SafeBoot
- WinMagic SecureDoc Full Disk Encryption
- PGP Whole Disk Encryption
- Checkpoint Full Disk Encryption

Supported Encryption Products

The table below shows encryption products supported by EnCase Decryption Suite and the credentials you need to provide to use them with EnCase Forensic.

Product	Password	Use-r	Domai-n	Machine	Serve-r	Path	Other
GuardianEdge Encryption Plus	X	X					
GuardianEdge Encryption Anywhere	X	X	X				
GuardianEdge Full Disk Encryption	X	X	X				
Utimaco SafeGuard Easy	X	X					
McAfee SafeBoot Online	X	X		X	X		Algorithm

Product	Password	User	Domain	Machine	Server	Path	Other
SafeBoot Offline				X		X	Algorithm
Dell Data Protection Enterprise/Credant Mobile Guardian Online	X	X		Machine Credant ID	X		Shield Credant ID
Dell Data Protection Enterprise/Credant Mobile Guardian Offline	X					X	
Microsoft BitLocker	X						Key
Microsoft Encrypting File System (EFS)	X						Keys
ZIP	X						
Lotus Mail	X						ID File
S/MIME	X						PFX
PGP Whole Disk Encryption	X					ADK requires path and passphrase	Passphrase, ADK, WDRT
FDE	X	X				Recovery file path	Challenge/ response

Product	Password	User	Domain	Machine	Server	Path	Other
WinMagic SecureDoc	Key file password					Key file path, Emergency disk folder path	

EDS Commands and Tabs

The following section details the various EnCase Decryption Suite commands and tabs.

Analyze EFS

The Analyze EFS command scans a volume for data and processes it. Alternately, you can run **Analyze EFS** from the secure storage, which consecutively scans all volumes in a case.

To run Analyze EFS:

1. Right click the volume you want to analyze, then click **Device** > **Analyze EFS** from the dropdown menu.
2. The first Analyze EFS dialog displays. Click **Next**.
3. The second Analyze EFS dialog displays with the Documents and Settings Path and Registry Path fields populated by default. For unusual system configurations, data disks, and other operating systems, these values are blank. You can modify them to point to the user profile folders and/or the registry path.
4. Click **Next** to begin the scan.
5. When the scan completes, the EFS Status dialog shows statistical information on keys found and decrypted and registry passwords recovered.
6. When you finish reviewing the EFS status, click **Finish**.

> **Note: Analyze EFS** can also open the Syskey and Password Recovery Disk screens.

MISSING IMAGES

If images that should have rendered display as blank, select the gear dropdown menu in Evidence view and click **Clear invalid image cache**.

Secure Storage Tab

To organize security data gathered using **Analyze EFS**, EnCase Forensic includes a **Secure Storage** tab which displays passwords, keys, and other items parsed from the system files and registry.

Although the tab is always present in the interface, the EDS module must be installed to enable most of the functionality.

Secure Storage Tab and EFS

To populate the **Secure Storage** tab:

1. Run Analyze EFS.
2. From the View dropdown menu, select **Secure Storage**.
3. Click an item in the Secure Storage tree to view its contents.

Enter Items

ENTER SYSKEY

You can enter Syskey information before running the Analyze EFS wizard, or afterwards if the wizard is already completed.

1. Click **View** > **Secure Storage**.
2. In the **Table** tab, click the hamburger icon, then click **Enter Items** from the dropdown menu.
3. Select the location of the Syskey or enter the password manually.
4. Click **OK**.

USER PASSWORD

If you know the user password:

1. In the **Table** tab, click the hamburger icon, then click **Enter Items** from the dropdown menu.
2. The Enter Items dialog opens to the **User password** tab.
3. Enter the password, then click **OK**.

If the Syskey is protected and you do not know the password, an attack on the SAM file for user passwords will fail. This is a rare situation. Most Windows machines do not have a

protected Syskey. EnCase Decryption Suite includes a dictionary attack option to get past a protected Syskey. You can obtain dictionary files from a number of sources. To open setup, right click the root of Secure Storage and select **Dictionary Attack**.

While Analyze EFS scans the registry, EnCase alerts you if the Syskey is password protected or has been exported. In these cases, the Analyze EFS wizard prompts you to enter the Syskey password or browse to the Syskey file location. The Syskey file is called `startkey.key`. You should examine any removable media collected at a scene for the presence of this file. If the Syskey file is recovered on removable media, it can be copied/unerased from EnCase to the examination machine, and you can browse to the `startkey.key` location. This process is the same as when you use the Password Recovery Disk.

PASSWORD RECOVERY DISK

Windows XP and 2003 Server enable local users to create a recovery disk with a file containing their encrypted passwords. The `userkey.psw` file allows users to reset their passwords, without losing all of their EFS encrypted files and other important security credentials. You should examine evidence recovered at the scene for the presence of this file.

1. With file on removable media, or copied to a hard drive, click the hamburger icon in the **Table** tab, then click **Enter Items** from the dropdown menu.
2. Select the **Password Recovery Disk** tab.
3. Click **File** or **Removable**.
4. Enter the path or browse to it, then click **OK**.

PRIVATE KEY FILE

If the logon password is unavailable, you can obtain the Domain Administrator's private key (PFX). This also works for a user key. To export and use the key:

1. As Domain Administrator, double click `C:\Windows\system32\certmgr.msc` to launch the Microsoft Management Console.
2. Locate the Certificates folder containing the Domain Administrator's certificate.
3. Right click the certificate.
4. From the All Tasks menu, click **Export**.
5. In the Certificate Export Wizard, click **Next**.
6. Click **Yes** to export the private key, then click **Next**.
7. Accept the default for the export file format, then click **Next**.
8. Select a path and name the key (this assigns a `.PFX` extension), then click **Next**.
9. When prompted, note the password entered.

   Note: The password cannot be left blank. It is needed when using the key.

10. Click **Next**. A confirmation window displays details about the export.
11. Click **Finish** to complete the export.

12. Click the hamburger icon in the **Table** tab, then click **Enter Items** from the dropdown menu.
13. In the Enter Items dialog, select the **Private Key File** tab.
14. Enter the path or browse to it.
15. Enter the Password in the next dialog, then click **OK**.

    A status screen confirms successful completion and the Private Key displays in the Secure Storage tab.

ENTER MAIL CERTIFICATE

You can enter a .PFX certificate to use for decrypting S/MIME-encrypted email found in PST files.

1. Click the hamburger icon in the **Table** tab, then click **Enter Items** from the dropdown menu.
2. In the Enter Items dialog, select the **Enter Mail Certificate** tab.
3. Enter the path to the `.PFX` certificate and the password.
4. Click **OK**.
5. The `.PFX` cert is decrypted and stored in Secure Storage.

Associate Selected

To associate *nix users with volumes:

1. Click **View** > **Secure Storage**.
2. Click the hamburger icon menu in the **Table** tab and click **Associate Selected...**.
3. The Associate dialog displays.
4. Expand the Volumes tree and select the volumes you want to associate.

Secure Storage Items

In the **Report** tab of the View pane, you can see details about the currently selected item in the Secure Storage. The Text and Hex views show the raw data. These items have the following properties:

- Name
- Encrypted
- Type
- Subtype
- Password
- Password Type

The following items are of interest:

- **Aliases**: Security Identifiers (SIDs) that point to one or more SID entities. They include a name and a comment.
- **Groups**: SIDs that point to one or more SID entities. They include a name and a comment. These are defined groups such as Administrators and Guests.
- **SAM Users**: Local Users; details are listed in the **Report** tab of the View pane.
- **Passwords**: Found and examiner added passwords.
- **Net Logons**: Local Users; details are listed in the **Report** tab of the View pane.
- **Nix User/Group**: Unix users/groups.
- **Lotus**: Lotus Notes.
- **Email Certificates**: Certificates used for S/MIME decryption and signature verification.
- **Disk Credentials**: Persistent key cache for disk/volume encryption products.
- **Master Keys**: A master key that protects every user's private key. The master key itself is encrypted with a hash of the user's Windows password.
- **Private Keys**: Keys used in the decryption of EFS files.
- **Internet Explorer (IE) Passwords**: Passwords from IE 6.
- **Policy Secrets**: LSA secrets which include the default password and passwords for services. Some of these secrets are not passwords but binary data placed there by the system and applications.
- **SAM Keys/Policy Keys/Dpapi/CERT**: Items for internal use.

Passware Integration

EnCase provides Passware v11.7 integration, which lets you export indexes and known passwords as a dictionary for decrypting protected files. Using this feature requires a valid installation of the Passware Kit.

EnCase can export data to Passware after processing evidence with the Evidence Processor and creating an index, or after running Analyze EFS. EnCase displays a warning if no index exists or if Analyze EFS was not previously run.

To export data to Passware:

1. Open a case with evidence.
2. Select **Tools** > **Passware Export**.
3. Click **Next**. A dialog displays, showing evidence and current status of data available for export to the Passware folder, including index words, hiberfil.sys files, EFS passwords, and registries.
4. Select by blue-checking the evidence required.
5. Browse to your preferred Passware Export Folder.
6. You can optionally add one file in the Extra Data field to be added to the Passware Export Folder.
7. Click **Finish**. EnCase displays a green progress bar and an Export Successful dialog when the exporting process completes.

EnCase creates a text configuration file for Passware that includes system information.

When you add additional words to the Passware dictionary list, EnCase exports the full dictionary list, overwriting previously exported data.

You can begin the export process alternately by right-clicking an evidence file entry, then selecting **Open with** > **Passware**.

The result is Passware displays data associated with the evidence file selected.

Configuring Passware as a Viewer

When you launch EnCase, if you have Passware installed, EnCase detects it. If it is not configured as a viewer, EnCase gives you the option to configure Passware as a viewer.

To configure the Passware viewer:

1. Right click an evidence item.
2. Select **Open with** > **File Viewers**. The Passware configuration dialog displays.

   Note: You must add [passwaredata] [file] to the Command Line field.

3. Click **OK**. Passware is now configured as a viewer.

Safeboot Encryption Support

EnCase provides a way for you to view SafeBoot encrypted hard drives during an investigation. This feature is available automatically to anyone using EnCase using the Export Restricted license flag. This flag needs to be enabled for strong encryption to take place. This feature is supported for the EnCase 32-bit platform only.

Additional SafeBoot support documentation is available at https://support.guidancesoftware.com/knowledge/node/1551.

Before running the Safeboot decryption:

1. Install the SafeBoot Installer from the Guidance Software Support Portal: https://support.guidancesoftware.com/forums/index.php?resources/categories/decryption-support.21/.

From the SafeBoot server, copy the following files to the locations indicated. The files on your SafeBoot Client machine (`c:\Program Files\SafeBoot`) do not work.

- **SBAlg.dll**: Copy to `C:\Program Files (x86)\EnCase\Lib\SafeBoot Technology\SafeBoot\sbAlgs`
  - Copy this file from the SafeBoot server under investigation.
  - Be sure this is the file that matches the algorithm selected during the server installation (the most common is AES-FIPS).
  - To verify the algorithm for a particular DLL, view the properties description. The corresponding SafeBoot algorithm can be referenced on the SafeBoot server by replacing the <algorithm> with the proper name based on the encryption algorithm that has been used to encrypt the drive. For example: If you are using the AES256 - FIPS algorithm, the path to the DLL file is: `C:\Program Files\SBAdmin\ALGS\AES256 - FIPS\SBAlg.dll`

- **SDMCFG.INI**: Copy to `C:\Program Files (x86)\EnCase\Lib\SafeBoot Technology\SafeBoot`
  - This file supplies the logon ID and password to use in case of an automated start.
  - It also contains a pointer to the port the server should speak on and its public and private key information. Make sure that this port is open so the server and clients can communicate.
  - This file is required for online usage and keeps the communication port open between SafeBoot server and clients.
  - The SafeBoot clients V5+ can send encrypted data to a V5 server.
  - V4 clients cannot send encrypted data to a V5 server, so for online use, change AuthType to zero in the .ini file so you can decrypt both V5 and V4 clients.
  - If you do not have or cannot get the SDMCFG.INI file, try creating a new empty text file with this name instead. It must be there to work (even if it is an empty file).

2. Restart EnCase.

Once these steps are completed, SafeBoot displays in the Help/About screen.

> **Note:** If the Export Restricted license flag is not enabled or the integration DLL files are not properly installed, the physical device mounts, but the encrypted file structure cannot be parsed. Since SafeBoot overwrites the original MBR for the boot disk only, always preview the boot disk first, then preview any other disk in a multi-disk machine configuration.

To acquire a SafeBoot encrypted device:

1. Use the Add Device wizard to add the physical device.
2. In the **Evidence** tab, click the device under the Name column.

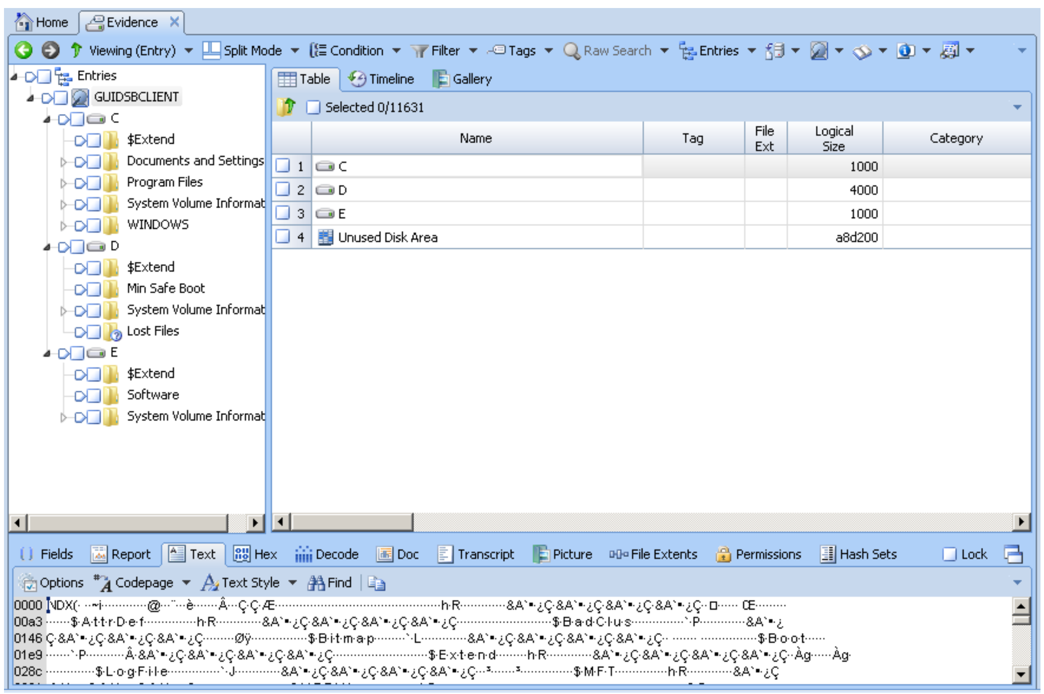
3. When prompted, select the appropriate encryption algorithm from the list, then, in online mode, enter a user name, server name, machine name, and password.

   The SafeBoot encrypted drive is parsed.

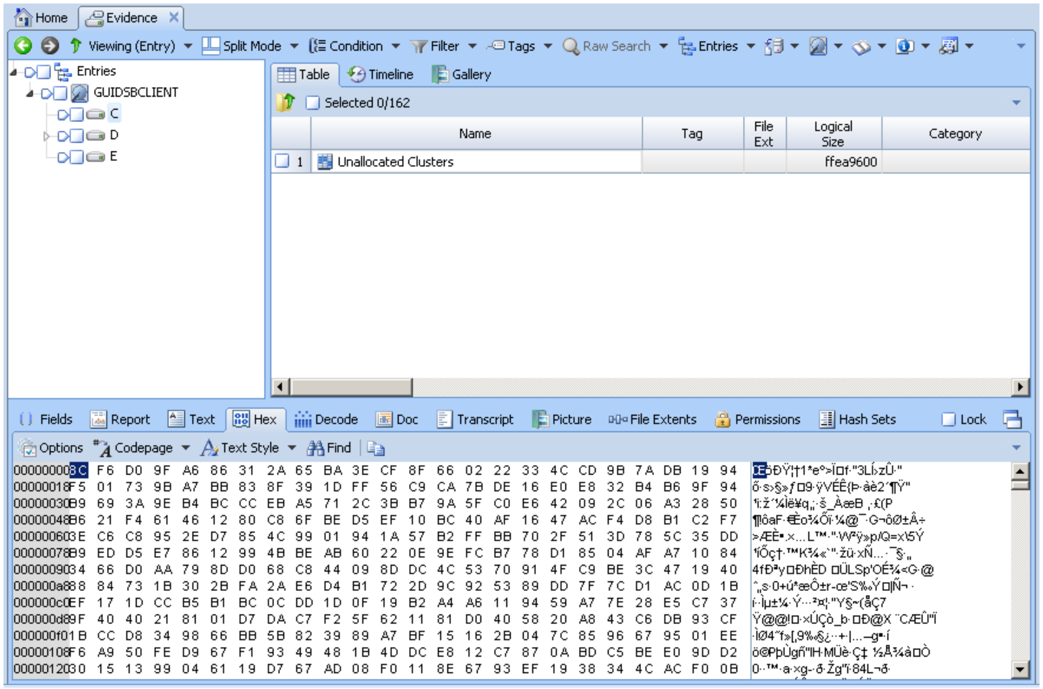
   The offline dialog is similar. The Online checkbox is blank and only the Machine Name, Transfer Database field, and Algorithm are available:

4. Save the case once a successful decryption is complete. The credentials entered in the dialog are stored in Secure Storage, eliminating the need to enter them again.

When a decryption is successful, the Tree pane shows a SafeBoot folder, the Table pane contains a list of decrypted files while the Text pane shows contents of a decrypted file.



The screenshot below shows the same files displayed as encrypted.



Note: The Safeboot encryption .dll causes EnCase to crash when the encryption algorithm for the server does not match the one implemented in SBAlg.dll.

Check Point Full Disk Encryption Support (Volume Encryption)

Check Point volume-based encryption supports the following two types of authentication:

- Username/password
- Challenge/response

When decrypting data that uses this form of encryption, begin as follows:

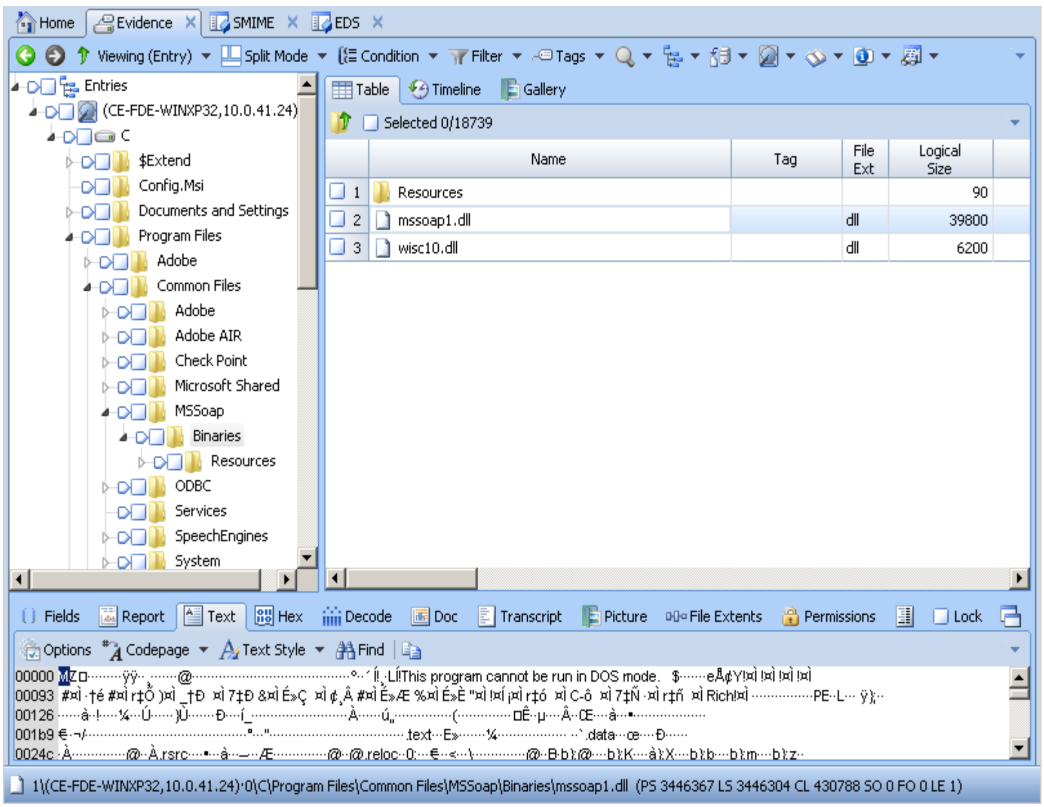
1. Add your evidence or preview the local disk that contains the Check Point encrypted volumes.
2. Go to the **Evidence** tab.
3. A dialog displays, prompting you for credentials. EnCase supports two types of authentication: username/password and challenge/response. EnCase determines which type of authentication is used based on the username you enter in the dialog.

Username and Password Authentication

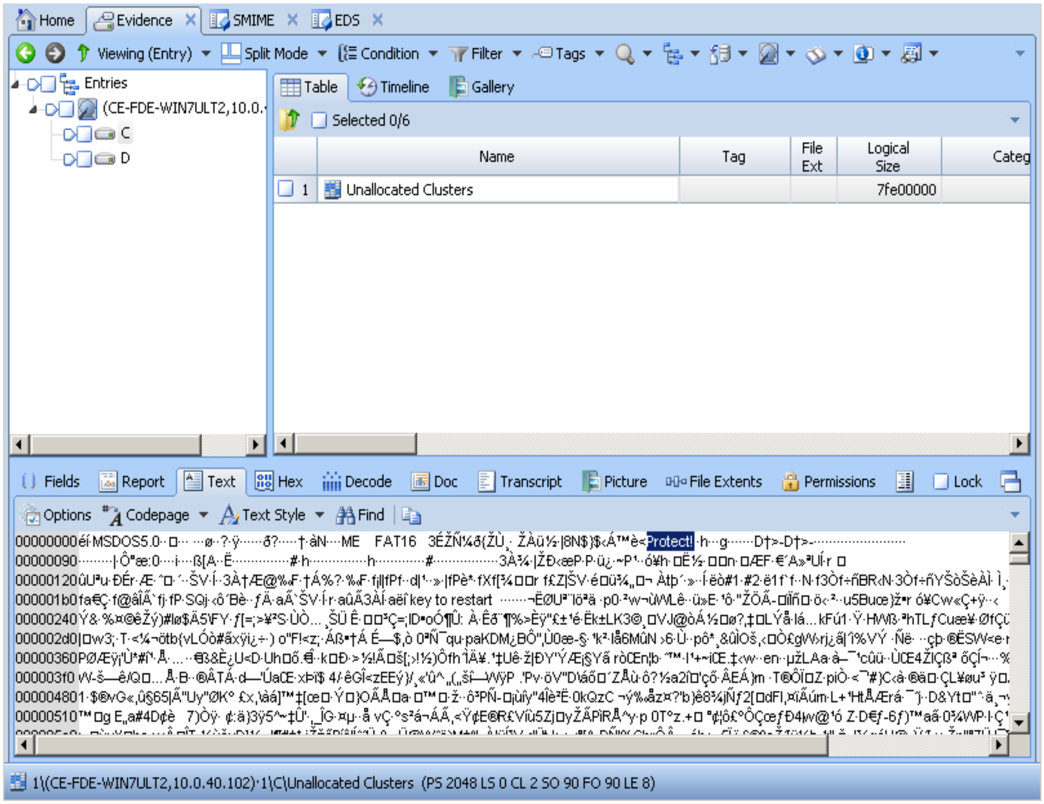
For username and password authentication:

1. Select **Evidence** > **Table**, and select a disk. A dialog displays showing the username and location of the recovery file path.
2. Click **Next**.
3. The Password Authentication dialog displays, with the password in the text field.
4. Click **Finish** to decrypt the selected disk.

The screenshot belowshows a successful decryption. Note the folder tree in the **Evidence** tab, and the DLL files listed in the **Table** tab.



If the decryption was unsuccessful or if the user canceled the dialog, this screen displays:

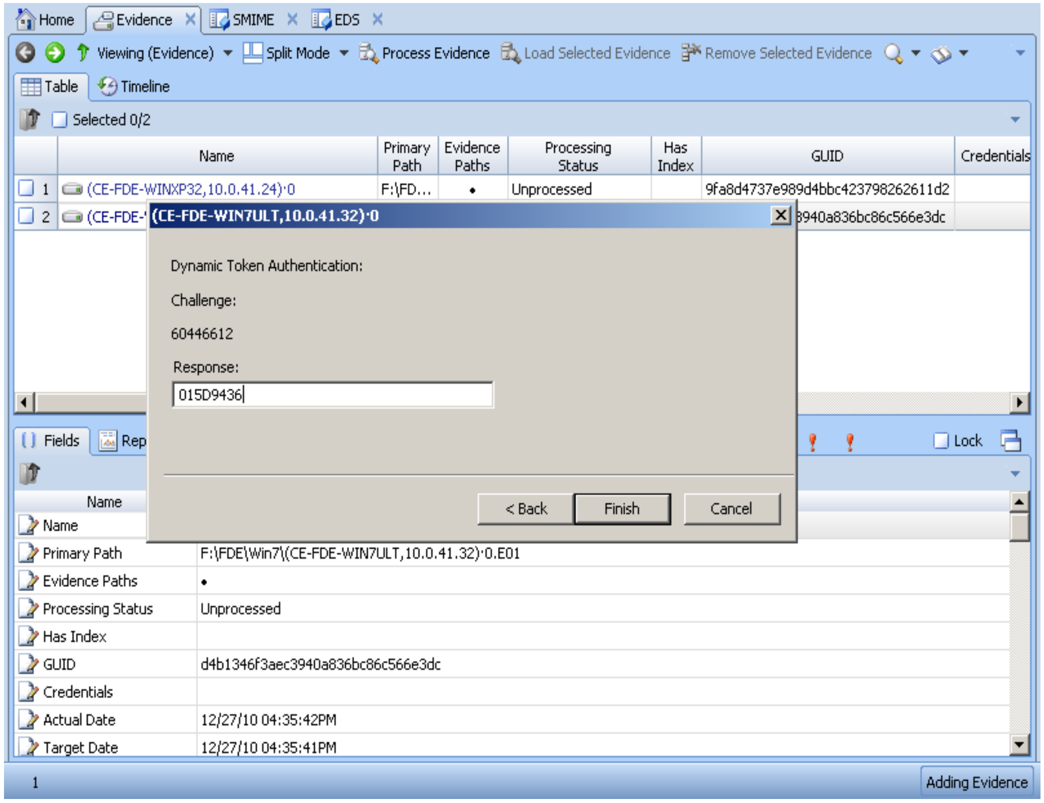


Note that the highlighted string "Protect!" in the View pane is a Check Point indicator that the disk is encrypted.

Challenge-Response Authentication

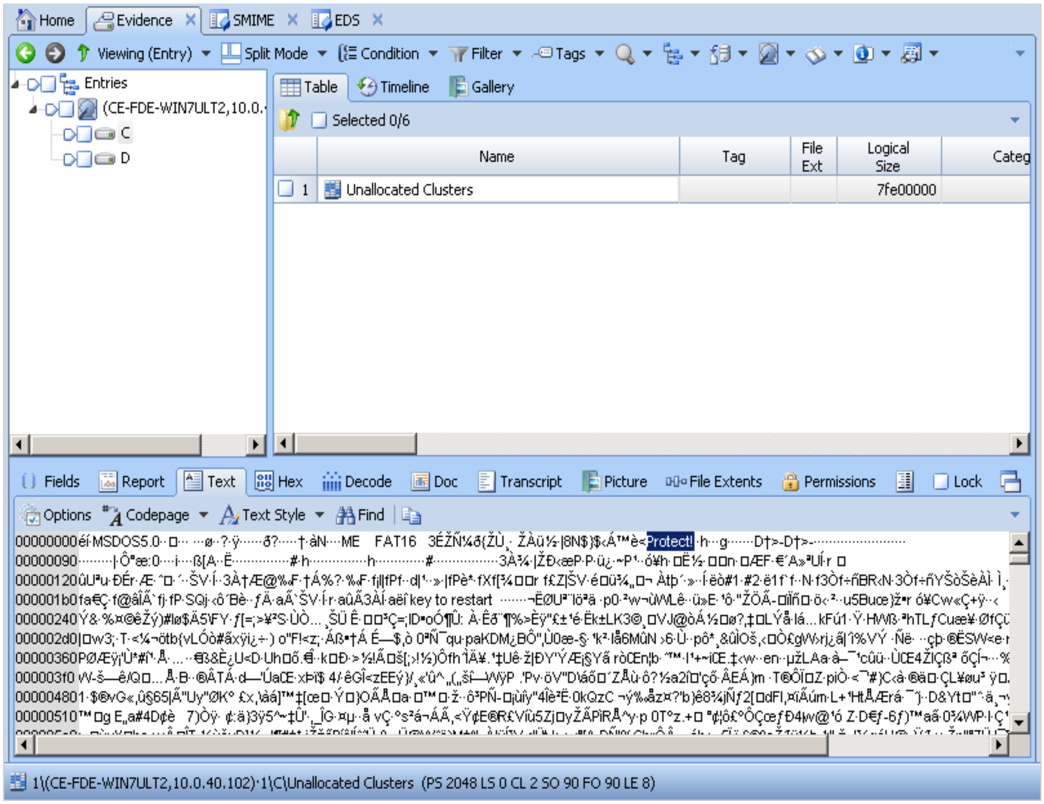
For challenge-response authentication:

1. Select **Evidence** > **Table**, and select a disk. A dialog displays showing the username and location of the recovery file path.
2. Click **Next**.
3. The following dialog indicates that the Challenge-Response form of Check Point Full Disk Authentication was used to encrypt the selected disk. Use the Check Point tool to generate a response for the challenge shown in the dialog. Copy the response value from the tool to the EnCase dialog.



4. Click **Finish**.

If the EnCase **Evidence** tab and the Table pane display as they do below, with no partitions, folders, or files visible, and if the "Protect!" string is visible in the View pane, then the decryption failed (or the user canceled the dialog). It is possible that the response is incorrect or that Check Point is unable to decrypt the selected disk.



BitLocker Encryption Support (Volume Encryption)

Microsoft BitLocker encrypts an entire volume using one of three modes to store the encryption key:

- Transparent operation mode (requires Trusted Platform Module [TPM])
- User Authentication mode (requires TPM)
- USB Key mode (does not require TPM)

When BitLocker is enabled, a large file is created that holds all unallocated (UAC) space, minus six gigabytes.

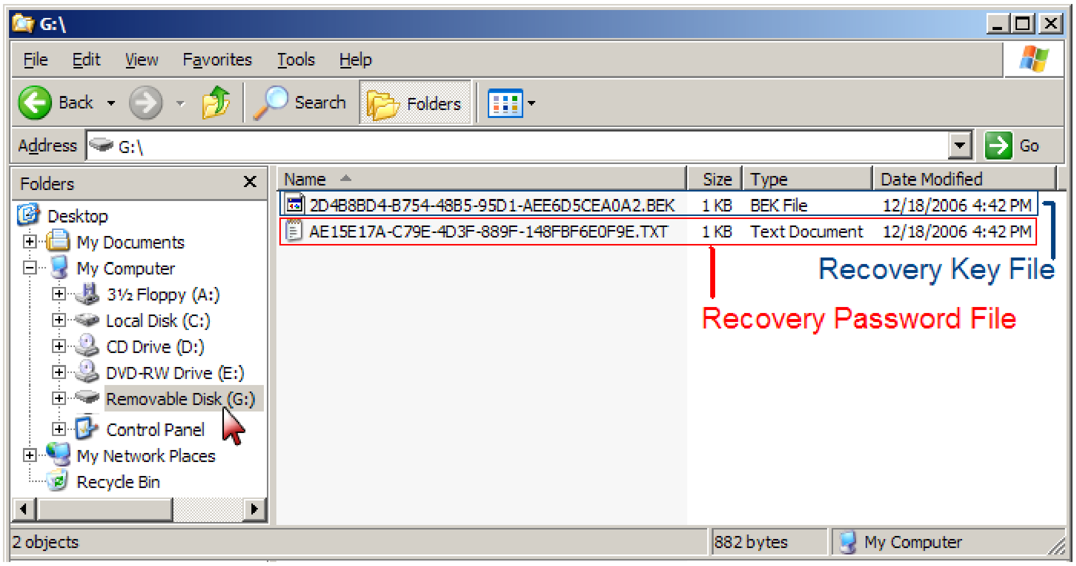
You can find a list of currently supported versions of BitLocker in your product's latest release notes.

Recovery Key and Recovery Password Files

The recovery key is a file with a GUID name (for example, 67FA3445-29D7-4AB5-8D0F-7F69B88D1C04.BEK).

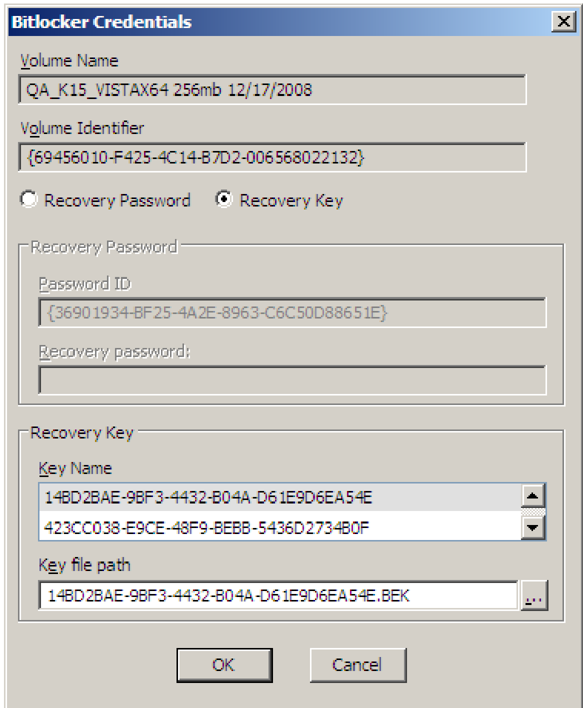
The recovery password is stored in a file with a GUID name (for example, AE15E17A-C79E-4D3F-889F-14FBF6E0F9E.TXT).

These keys are matched by Key Protector GUID in the BitLocker metadata.

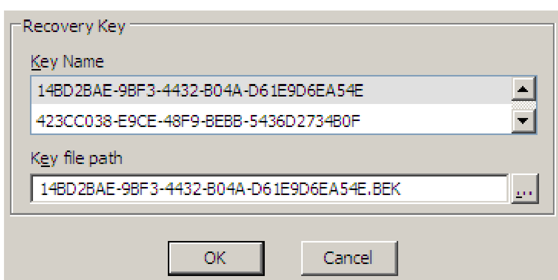


Decrypting a BitLocker Encrypted Device Using Recovery Key

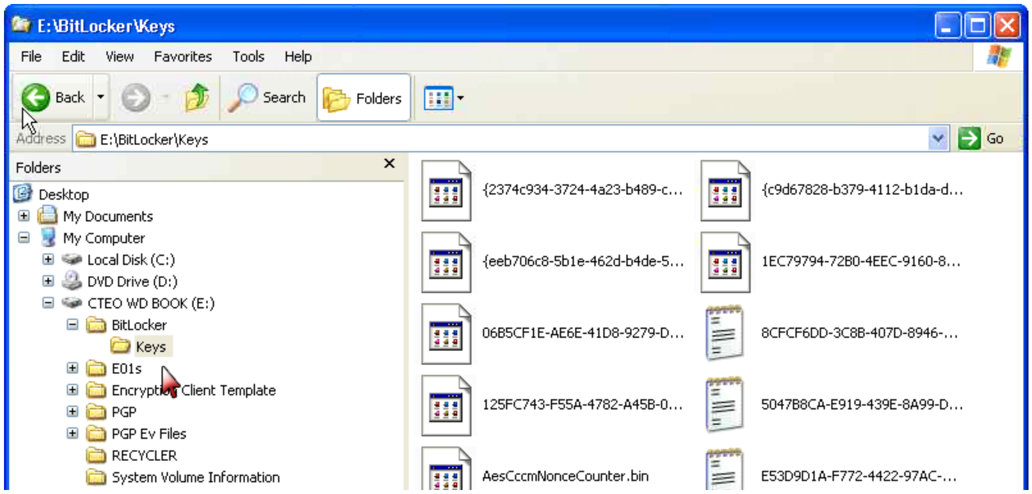
1. Add a BitLocker encrypted device into EnCase using **Add Device** or drop and drag.
2. The BitLocker Credentials dialog displays.



3. The **Recovery Key** option button is selected by default. Browse to the location of the required .BEK recovery key.



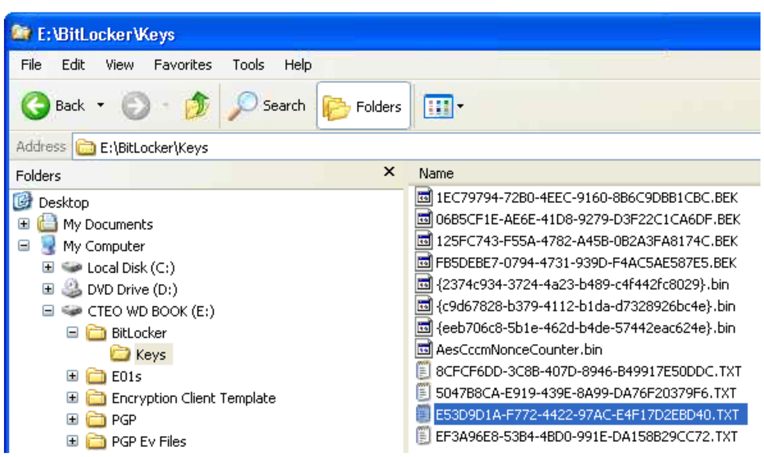
4. Browse to the folder containing BitLocker keys and select the specified .BEK file.

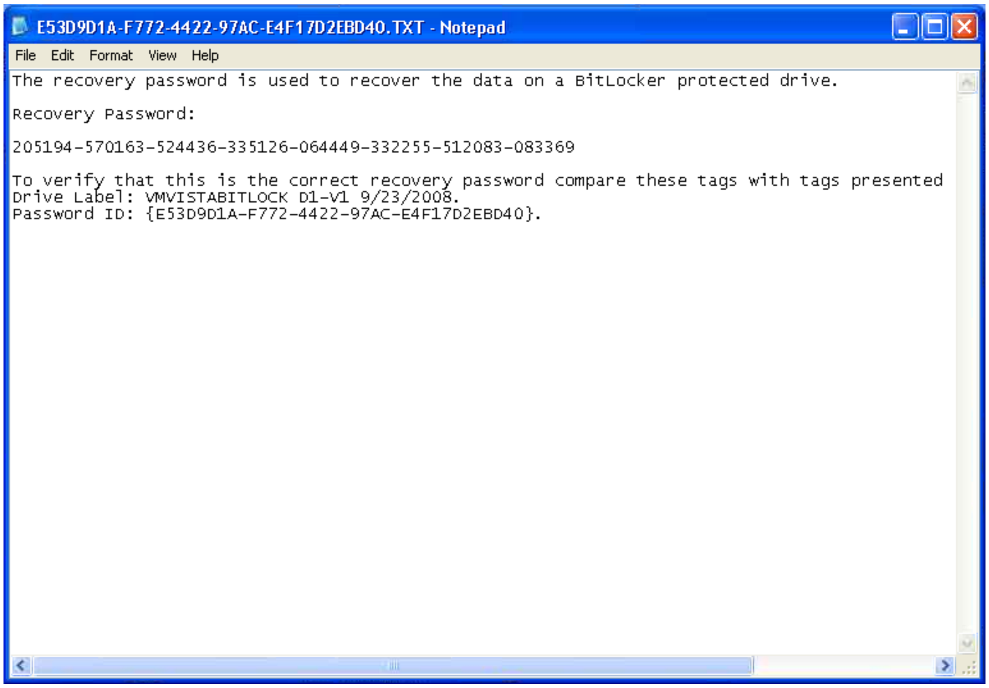


5. Click **OK**.

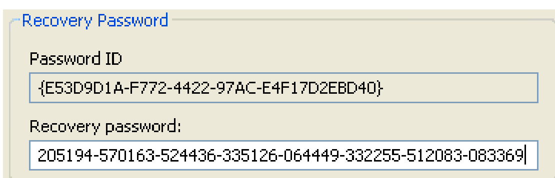
Decrypting a BitLocker Encrypted Device Using Recovery Password

1. Add a BitLocker encrypted device into EnCase using **Add Device** or drop and drag.
2. The BitLocker Credentials dialog displays.
3. Select the **Recovery password** option button.
4. Browse to the folder containing BitLocker keys.
5. Find and open the .TXT file that matches the Password ID.





6. Copy and paste the recovery password into the BitLocker Credentials dialog.



7. Click **OK**.

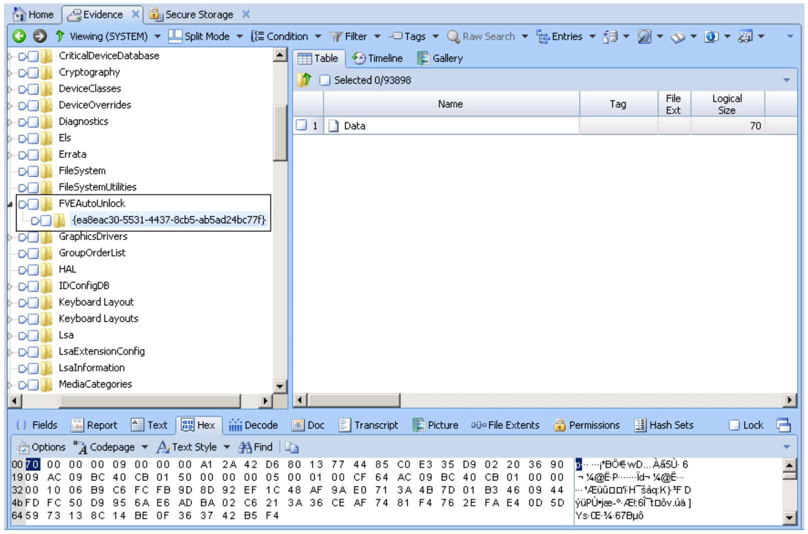
Full Volume Encryption (FVE) AutoUnlock Mechanism

Encrypted data volumes are decrypted on the fly; that is, the sectors belonging to the volume are automatically decrypted and the file system parsed, without any user intervention, given that the boot volume was successfully decrypted by:

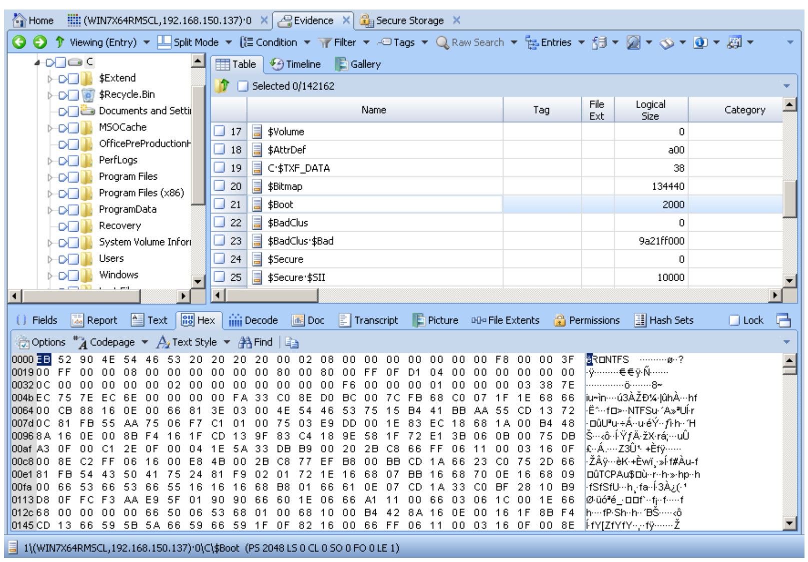
- Providing a valid recovery key or recovery password
- Running **Analyze EFS** on the decrypted boot volume

Each data volume has a corresponding registry key (`SYSTEM\ControlSet0xx\FVEAutoUnlock\{GUID}`) containing the key (AutoUnlock Volume Key, or AUVK) that can decrypt the Volume Master Key of that particular volume. This key has an associated GUID matching the GUID of a key protector in the data volume metadata.

The following displays AutoUnlock registry keys for three volumes:



The following displays Secure Storage after the **Analyze EFS** process:



Physical RAID Encryption Support

BitLocker supports physical RAIDs only, not logical RAIDs.

RAID 1: EXAMPLE USING TWO PHYSICAL DRIVES

1. Add a BitLocker encrypted primary RAID 1 volume into EnCase using **Add Device** or drop and drag. This primary volume consists of:
   - The boot disk
   - The BitLocker volume (which is not encrypted)
2. The BitLocker Credentials dialog displays.
3. Provide the credentials. See Decrypting a BitLocker Encrypted Device Using Recovery Key on page 668 or Decrypting a BitLocker Encrypted Device Using Recovery Password on page 670 for details.
4. Click **OK**. EnCase decrypts the volume.
5. Add each additional physical disk in order, repeating steps 2-4 for each disk, as needed.

   Note: For information on acquiring and building RAIDs, see How to Acquire RAIDs (https://support.guidancesoftware.com/knowledge/node/100) on the Guidance Software Support Portal.

RAID 5: EXAMPLE USING THREE PHYSICAL DRIVES

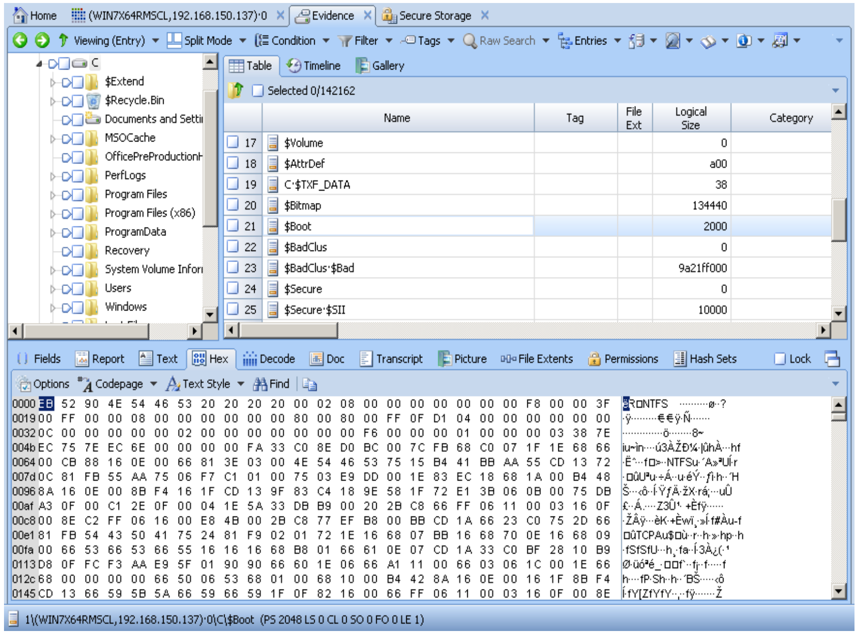
To parse a RAID 5 drive, you must first build the RAID in EnCase.

1. Add a BitLocker encrypted primary RAID 5 volume into EnCase using **Add Device** or drop and drag. This primary volume consists of:
   - The boot disk
   - The BitLocker volume (which is not encrypted)
2. Add each additional physical disk using **Add Device** or drop and drag.

   Note: The BitLocker Credentials dialog does not display until you finish building the RAID. For information on acquiring and building RAIDs, see How to Acquire RAIDs (https://support.guidancesoftware.com/knowledge/node/100) on the Guidance Software Support Portal.
3. When you finish building the RAID, EnCase displays the BitLocker Credentials dialog.
4. Provide the credentials. See Decrypting a BitLocker Encrypted Device Using Recovery Key on page 668 or Decrypting a BitLocker Encrypted Device Using Recovery Password on page 670 for details.
5. Click **OK**. EnCase decrypts all available volumes.

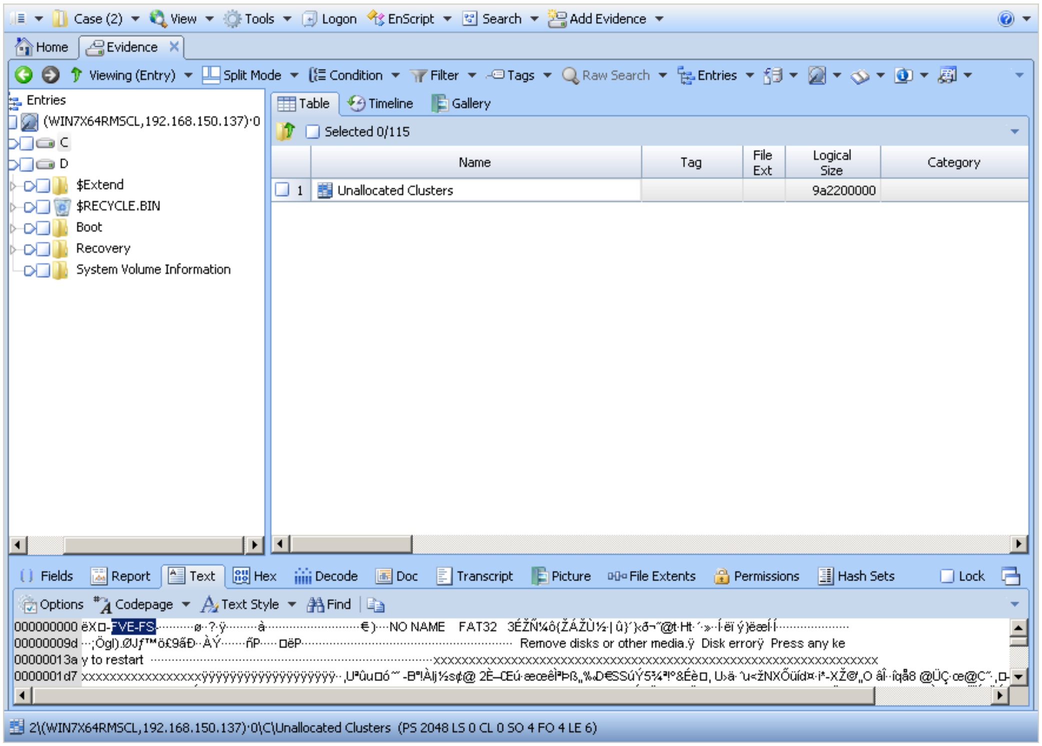
Successful BitLocker Decryption

When decryption is successful, the volume's file system type displays in the first sector.



Unsuccessful BitLocker Decryption

If decryption fails, **FVE-FS** displays in the first sector.



Saved BitLocker Credentials in Secure Storage

After successful authentication, EnCase saves credentials in Secure Storage, so you do not have to re-enter them the next time you open the saved case.

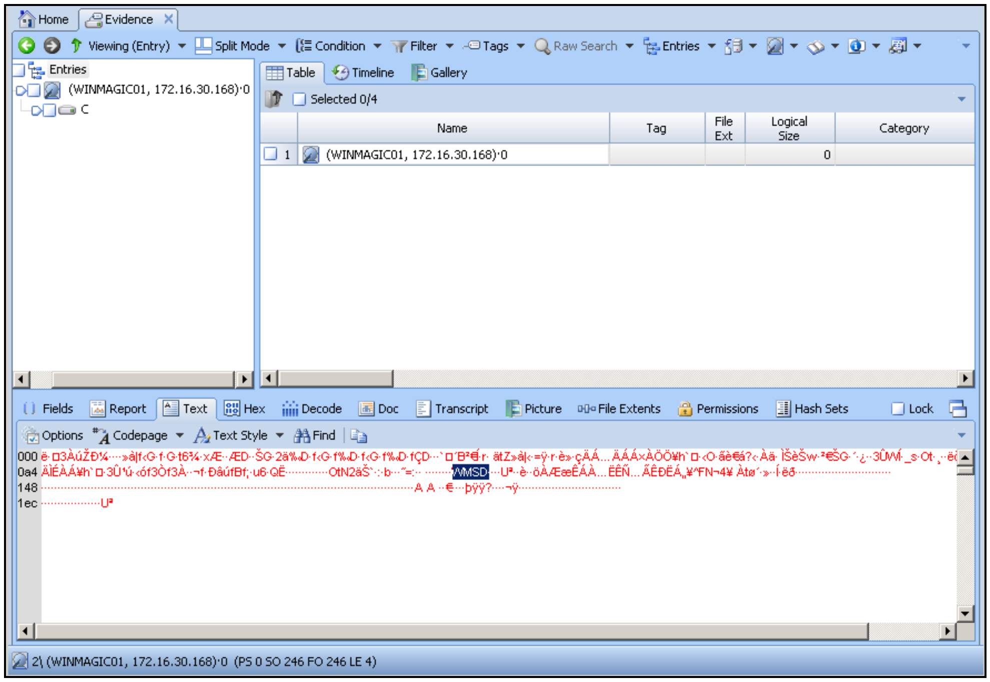
WinMagic SecureDoc Encryption Support

With SecureDoc software, you can access the hard drive of an encrypted system.

There are three ways to add SecureDoc disks to EnCase:

- Preview the hard drive
- Use the Add Device wizard
- Drag evidence files into EnCase

When you preview a machine's disk or open an evidence file, the Master Boot Record (MBR) is checked against known signatures to determine whether the disk is encrypted. The SecureDoc signature is **WMSD**.



Each SecureDoc user has a key file which can contain multiple keys encrypted using a password associated with the file.

SecureDoc users have either administrator or user privileges:

- Administrators can encrypt/decrypt drives, reset passwords, add keys to a key file, etc.
- Users can change their passwords only.

An installer is provided to place these integration DLL files in `%ENCASE%\Lib\WinMagic\SecureDoc`:

- SDForensic.dll
- SDC.dll
- SDUser.dll

Note: The 32-bit version of EnCase supports the integration.

1. When adding a SecureDoc disk, Encase prompts for three credentials:
    - The path to the file containing the user keys (extension .dbk).
    - The password associated with the key file.
    - The path to the emergency disk folder corresponding to the physical disk under examination.

2. Enter the credentials, then click **OK**.
3. If the credentials are correct, EnCase decrypts the disk and parses the file system structure.
4. When you save the case, the ranges of encrypted sectors and the original MBR are retained in the case file for previewed drives as well as evidence files.

The disk view shows encrypted information in the Text and Hex panes for encrypted drives.

ACQUIRING THE DEVICE

A local acquisition at the physical device level results in acquisition of all decrypted logical volumes, when the correct credentials are provide.

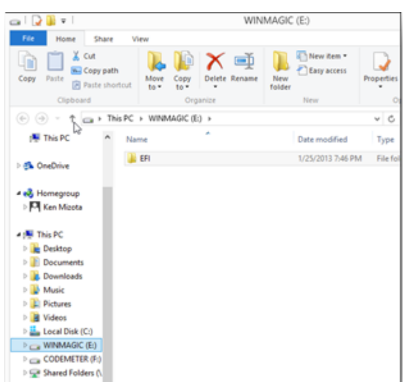
> **Note:** To obtain decrypted data, perform a local acquisition on the result of the remote acquisition by providing the correct credentials.

The completed acquisition contains the decrypted sectors.

WinMagic SecureDoc Self Encrypting Drive (SED) Support

You can unlock and decrypt SED drives in EnCase using WinMagic.

1. Connect a WinMagic SecureDoc managed SED to the forensic workstation. Only the 128MB Master Boot Record shadow file system is available to the OS.



2. Add the physical device to your case in EnCase.
3. Open the device and enter your SecureDoc credentials when prompted.
4. Click **OK**. EnCase parses the file system, and the SED is unlocked and presented to EnCase (but it is still invisible to the OS).

> **Note:** Self encrypting drives cannot be unlocked if the drive has been write blocked.

GuardianEdge Encryption Support

EnCase supports the following GuardianEdge products:

- GuardianEdge Encryption Plus
- GuardianEdge Encryption Anywhere
- GuardianEdge Hard Disk Encryption, versions 9.2.2 through 9.5.1

To decrypt, you need a cert file for your dongle to activate the EDS module in EnCase.

For Encryption Plus/Encryption Anywhere you will need:

- The EPCL32.dll file placed in the \lib\PC Guardian-Guardian Edge\EPHD folder in your EnCase installation.
- The EPcrypto.dll file placed in the \lib\PC Guardian-Guardian Edge\EPHD folder in your EnCase installation.
- Username
- Password

For Hard Disk Encryption/Encryption Anywhere you will need:

- The EPCL32.dll file placed in the \lib\PC Guardian-Guardian Edge\EAHD folder in your EnCase installation.
- The EAECC.dll file placed in the \lib\PC Guardian-Guardian Edge\EAHD folder in your EnCase installation.
- Username
- Password
- Domain

Upon previewing an encrypted device or adding a physical evidence file of an encrypted device, EnCase prompts for the credentials. Once the correct credentials are added, the file and folder structure of the device displays unencrypted.

EnCase also supports decryption for Symantec Endpoint Encryption, the successor product to GuardianEdge encryption products. To view supported versions of Symantec Endpoint Encryption, see Symantec Endpoint Encryption Support on page 681.

Supported GuardianEdge Encryption Algorithms

EnCase GuardianEdge decryption supports these encryption algorithms:

- AES128
- AES256

GuardianEdge Hard Disk and Symantec Endpoint Encryption Support

EnCase supports the following versions of Guardian Edge Hard Disk (GEHD) and corresponding versions of Symantec Endpoint Encryption (SEE):

- GEHD 9.5.1 and SEE 7.0.6
- GEHD 9.5.0 and SEE 7.0.5
- GEHD 9.4.0 and SEE 7.0.4
- GEHD 9.3.0 and SEE 7.0.3
- GEHD 9.2.2 and SEE 7.0.2

> **Note:** Affected dialogs which previously displayed the text "GuardianEdge" now show it as "GuardianEdge/Symantec."

If EnCase Reports GuardianEdge/Symantec dlls Cannot be Opened

If EnCase reports that GuardianEdge/Symantec EAHD DLL files could not be opened when attempting to decrypt a SEE device from a Windows 7 or Windows 8 x86 operating system or a Windows Vista x64 operating system, be sure 32-bit and 64-bit DLL files are installed that match the examiner machine: a 32-bit examiner machine requires 32-bit DLL files, and a 64-bit examiner machine requires 64-bit DLL files.

The following DLL files are required to decrypt an SEE encrypted device on a 32-bit examiner machine:

- `EAECC.dll`
- `EPCL32.dll`

The following DLLs files are required to decrypt an SEE encrypted device on a 64-bit examiner machine:

- `EAECC.dll`
- `EPCL.dll`

Place these DLLs files in the `Lib\PC Guardian-Guardian-Edge\EAHD` folder of your EnCase installation.

> **Note:** The version of the EAECC.dll must match the product version of SEE.

In addition to the above, you may need to install the following if they are not already present on the system:

- GEHD 9.4.1/SEE 7.0.4: `msvcp71.dll` and `msvcr71.dll`
- GEHD 9.5.0/SEE 7.0.5: `msvcp80.dll` and `msvcr80.dll` (these must match the EnCase platform: 32 or 64-bit)
- GEHD 9.5.1/SEE 7.0.6: `msvcp80.dll` and `msvcr80.dll` (these must match the EnCase platform: 32 or 64-bit)

You can obtain the DLL library you need from the SEE installation folders on the client machine.

AUTHENTICATING A PHYSICAL DRIVE IN ENCASE

Because GEHD has domainless client administrators, you need to use a default field for the domain:

1. Make sure you have the EnCase Decryption Suite module with PC Guardian support installed. Check by selecting **Help > About...**.
2. In the domain field, enter EA#DOMAIN as the client administrator account.

DECRYPTING A GUARDIANEDGE ENCRYPTED DEVICE RUNNING ENCASE ON A VISTA OPERATING SYSTEM

If you use EnCase on a Windows Vista operating system to decrypt a GuardianEdge encrypted device, you need the following DLL files in the EnCase8\lib directory.

For GuardianEdge Encryption Anywhere and GuardianEdge Hard Disk Encryption:

```
PC Guardian-Guardian Edge\EAHD\EAECC.dll
PC Guardian-Guardian Edge\EAHD\EPCL32.dll
PC Guardian-Guardian Edge\EAHD\msvcp71.dll
PC Guardian-Guardian Edge\EAHD\msvcr71.dll
```

For GuardianEdge Encryption Plus:

```
PC Guardian-Guardian Edge\EAHD\EPCL32.dll
PC Guardian-Guardian Edge\EAHD\EPcrypto.dll
```

USING GUARDIANEDGE OVERALL AUTHORITY

This applies to GuardianEdge version 8 and higher.

If you are using a GuardianEdge Overall Authority (GEOA) account, you must use EA#DOMAIN for the domain.

Note: This does not apply to GuardianEdge Encryption Plus.

Symantec Endpoint Encryption Support

EnCase provides decryption support for Symantec Endpoint Encryption 8.0 and 7.0.2 through 7.0.6.

Symantec Endpoint Encryption is a successor product to GuardianEdge encryption products. To view supported versions of GuardianEdge, see GuardianEdge Encryption Support on page 678.

Symantec Endpoint Encryption v11.1.1 support

EnCase Forensic supports the decryption of files that have been encrypted with Symantec Endpoint Encryption v11.1.1.

To use this functionality:

1. In your browser, navigate to the Symantec downloads page: http://www.symantec.com/connect/downloads/pgp-sdk
2. Download these two files:
    - `PGPsdk.dll`
    - `PGPsdk.dll.sig`
3. Navigate to your Symantec Endpoint Encryption installation folder: `\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\PGPce.dll and PGPce.dll.sig`
4. Locate these two files:
    - `PGPce.dll`
    - `PGPce.dll.sig`
5. Place these four files in your EnCase installation folder: `[Encase_Installation_Dir]\Lib\PGP\WDE`

Once these files are added to the correct folder, you can decrypt evidence encrypted with Symantec Endpoint Encryption v11.1.1.

Sophos SafeGuard Support

EnCase provides the following support for Sophos SafeGuard Enterprise (Sophos SGN) and Easy Versions 5.50 and 5.60:

- Partition/volume-based encryption support
- AES128 and AES256 support
- Support for Windows only
- Support in EnCase x86 only

To use Sophos SGN, you must obtain keys from a forensic administrator.

Decrypting a Disk

To decrypt a disk containing Sophos SGN encrypted partitions:

1. Open the SafeGuard Management Center to create a virtual client on the Sophos SGN server.
2. The SafeGuard Management Center displays.
3. Select the **Keys and Certificates** option from the left navigation pane.
4. The Keys and Certificates section displays.
5. Under **Keys and Certificates** select **Virtual Clients**.
6. Virtual Clients displays in the right pane.
7. Select **Actions** > **Add Virtual Client**.
8. The New Virtual Client dialog displays.
9. Enter a name in the Name field and click **OK**.
10. The new virtual client name (EnCaseVirtualClient) displays in the right pane.
11. Select the new virtual client (EnCaseVirtualClient) in the right pane.
12. Select **Actions > Export Virtual Client**.
13. Select and save the new virtual client.
14. Copy the new virtual client to the Examiner machine.

Decrypting Sophos SGN-Encrypted Evidence Using a Challenge/Response Session in EnCase

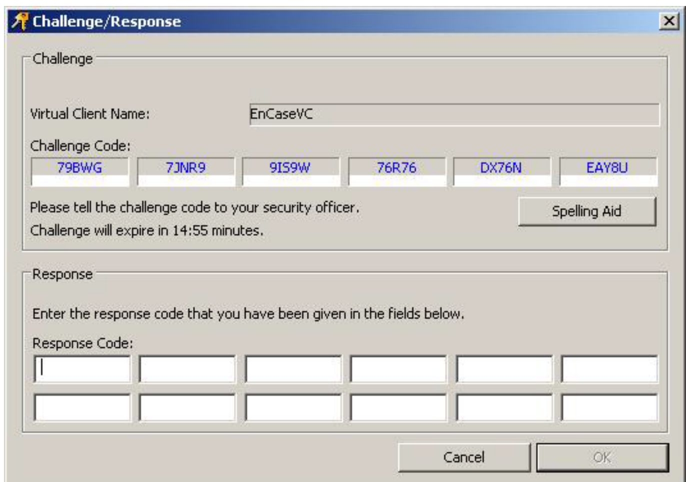
On the EnCase Examiner machine, EnCase detects whether the current device contains partitions encrypted with Sophos SGN.

To decrypt SGN-encrypted evidence using a Challenge/Response session:

1. In the **Evidence** tab double click the evidence name.
2. The Virtual Client Recovery Token File dialog displays.
3. Browse to the virtual client recovery token file (recoverytoken.tok) exported from the Sophos SGN server.
4. The keys (KEKs) encrypting the data encryption key (DEK) of the current partition display.
5. Select a key ID and click **OK**.

   A Challenge/Response session is initiated to get the plain KEK whose ID was selected previously from the Sophos SGN server.

6. The EnCase Challenge/Response dialog displays.



To populate the EnCase Challenge/Response dialog with data obtained from the Sophos SGN website, complete the steps described in the following section.

The plain DEK of the partition is derived from the KEK obtained previously thus decrypting the sector data.

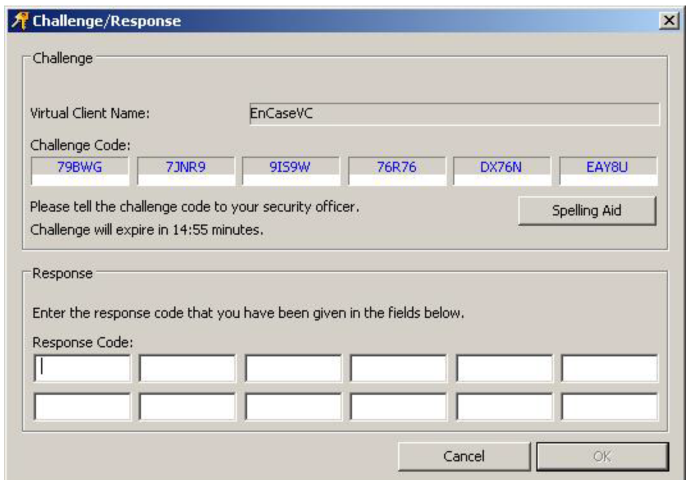
Obtaining Response Codes from the Sophos SGN Website

Sophos SGN provides a Web site where forensic administrators can carry out Challenge/Response sessions.

To obtain the response codes from the Sophos SGN website:

1. Open a web browser.
2. Navigate to the Sophos SGN website.
3. The Sophos SGN Authentication dialog displays.
4. Enter your security officer ID and password, and click **Log on**.

5. The Recovery type dialog displays.
6. Select **Virtual Client**, then select the virtual client that was provided to EnCase (recov-erytoken.tok). Click **Next**.
7. The Select Virtual Client action dialog displays.
8. Select **Key requested**, then click **Next**.
9. The Select key/key file for Virtual Client recovery dialog displays.
10. Click the browse icon and select the key based on your previously selected key ID in EnCase, then click **Next**.
11. The Enter challenge for Virtual Client dialog displays.
12. Enter the challenge codes from the EnCase Challenge/Response dialog in the challenge fields.



13. Click **Next**.
14. The Challenge/Response data window displays.
15. Sophos SGN generates and displays the required response codes.

Completing the Challenge/Response Session

To complete the challenge/response data acquisition process:

1. Return to the EnCase Challenge/Response dialog and enter the response codes obtained from the Sophos SGN website in the Response Code fields.
2. Click **OK** to complete the challenge/response data collection process.
3. The plain DEK identified by the selected key ID is returned.

Utimaco SafeGuard Easy Encryption Support

EnCase provides a way to view SafeGuard Easy (SGE) encrypted hard drives during an investigation. This feature is available only to a user with the Export Restricted license flag enabled. **Note**: If the Export Restricted license flag is not enabled or the integration DLL files are not properly installed, the physical device mounts, but the encrypted file structure cannot be parsed. Since SafeGuard Easy overwrites the original MBR for the boot disk only, only the boot disk can be decrypted in EnCase.

1. Use the Add Device wizard to add the physical device.
2. EnCase detects the device and displays a username and password dialog.
3. In online mode, enter a valid username and password.
4. Click **OK**.
5. Once a successful decryption is complete, save the case. The credentials entered in the dialog are stored in Secure Storage, eliminating the need to enter them again.

Note: If the password is empty, the Challenge/Response wizard opens. For more information, see Utimaco Challenge/Response Support below.

Supported Utimaco SafeGuard Easy Encryption Algorithms

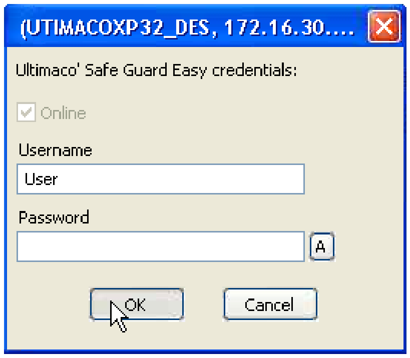
The EnCase Utimaco SafeGuard Easy decryption feature supports these encryption algorithms:

- AES192
- AES256
- DES
- 3DES

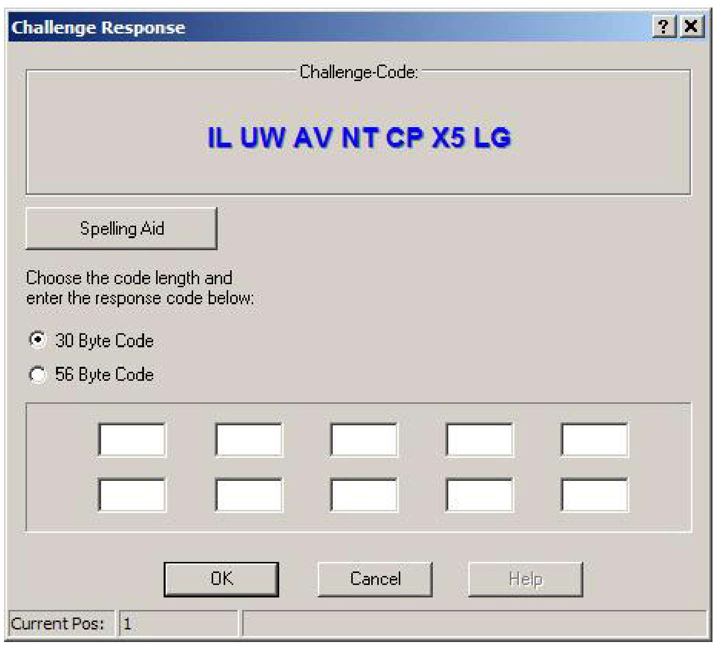
Utimaco Challenge/Response Support

Utimaco has an alternate method for decrypting data using a challenge/response code. Once the code is authenticated, EnCase returns the key and any additional data (such as encrypted sectors) necessary to decrypt the data.

1. In the SGE credentials dialog, enter a username but leave the password field blank.

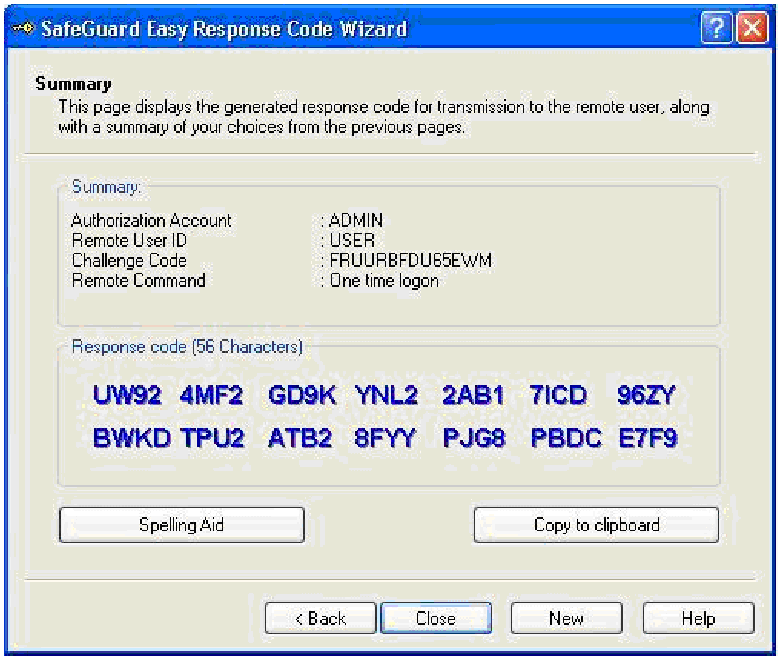


2. Click **OK**.
3. A Challenge Response dialog displays with the challenge code in blue/bold font. Keep this dialog open while performing the next steps.

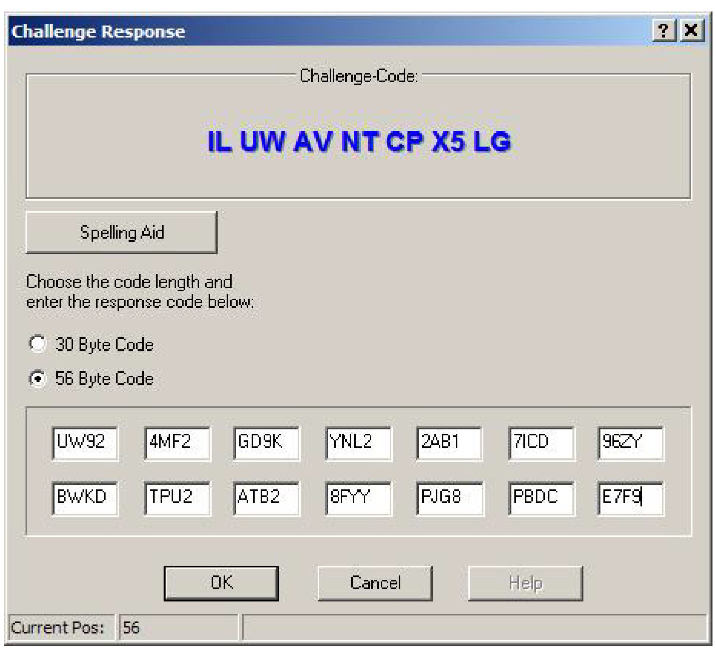


4. Log in as Administrator. Click the Windows **Start** button, then click **All Programs > Utimaco > SafeGuard Easy > Response Code Wizard**.
5. The Welcome dialog displays.
6. Click **Next** to begin generating a one time password (OTP). The Authorization Account dialog displays.
7. Click **Next**. The Remote User ID dialog displays.
8. Enter the User ID that was used to derive the challenge code, then click **Next**.
9. The Challenge Code dialog displays. Enter the challenge code generated by EnCase from step 3.

10. Click **Next**. The Remote Command dialog displays.
11. Select **One time logon**, then click **Next**.
12. The Summary dialog displays with the response code displayed in blue/bold font.



13. In the EnCase dialog from step 3, select the code length and enter the response code to enable decryption of the selected encrypted evidence.



14. Click **OK**.
15. In the Summary dialog from step 12, click **Close** to close the SafeGuard Easy Response Code Wizard, or click **New** to generate a new response code from a different challenge code.

Utimaco SafeGuard Easy Encryption Known Limitation

Utimaco SafeGuard Easy treats a machine with multiple hard drives as one hard drive consisting of all sectors of all physical hard drives.

In contrast, EnCase examines each hard drive individually. This creates a problem:

- SafeGuard Easy overwrites the Master Boot Record (MBR) of the boot disk only.
- Only the boot disk is detected as encrypted and then decrypted (when the correct credentials are entered).

This means EnCase support for SafeGuard Easy is limited to decrypting only the boot disk, because this is the only drive detected as encrypted by examining the MBR.

WORKAROUNDS

There are two workarounds for this problem.

The first workaround:

1. Obtain both disks.
   - The internal disk holding the SafeGuard Easy kernel (disk 1).
   - The external (that is, non-bootable) disk (disk 2).
2. Open the kernel on disk 1.

You have access to disk 2.

The second workaround:

1. Obtain a SafeGuard Enterprise (SGN) kernel backup file of disk 1.
2. Restore disk 1 to an empty disk.
3. Add the non-bootable disk as disk 2.

The information in the newly restored kernel gives you access to disk 2.

PGP Whole Disk Encryption (WDE) Support

Supported software versions and platforms include:

- PGP 9.8 or later
- Windows Vista (all 32 and 64-bit versions)
- Windows XP (SP1 and SP2)
- Windows 2000 Professional (SP4)
- Mac OS 10.4, 10.5, and 10.6

To decrypt a PGP encrypted disk, you need one of the following:

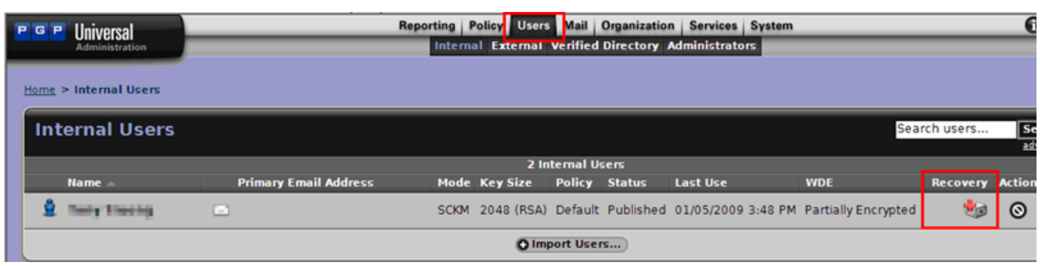
- A Whole Disk Recovery Token (WDRT) from the PGP Universal Server
- An Additional Decryption Key (ADK) from the client machine
- The user's passphrase

> **Note:** The `PGPEnCase.dll` resides in the installation folder of EnCase (typically `C:\Program Files\EnCase8\lib\PGP\WDE`). When using ADK authentication, the `PGPEnCase.dll` should be copied to the same location.

Obtaining Whole Disk Recovery Token Information

1. Open a browser and enter the PGP Universal Server's URL to gain access to the PGP Universal Administration page. The URL address displays in the PGP Universal Server boot screen.

2. Click the **Users** tab to go to the Internal Users page. Note which user displays the Recovery icon associated with a user name.



3. Click the user name associated with the Recovery icon. The Internal User Information page displays.
4. Click the **Whole Disk Encryption** button to see the machine associated with this user.
5. Click the **WDRT** icon.
6. The Whole Disk Recovery Token page displays. Note the token key consisting of 28 alphanumeric characters.
7. In EnCase, enter the token key in the Whole Disk Recovery Token field of the PGP Whole Disk Encryption credentials dialog, then click **OK**.

Note: You can enter the token key with or without dashes.

Obtaining Additional Decryption Key (ADK) Information

Note: The Additional Decryption Key option is available only with the EnCase x32 bit installer.

1. Log on to the PGP client workstation.
2. Click **Start > Programs > PGP > PGP Desktop**.
3. Locate the PGP SDK. Select it and drop it into the same folder as PGPEnCase.dll.
4. In the PGP Desktop - PGP Disk window, click **PGP Disk** on the left and select any disk listed.
5. The Disk Properties display.
6. In the User Access section at the bottom of the window, export the key as an .asc file.
7. In EnCase, in the **PGP Whole Disk Encryption credentials** dialog, enter the full path to the .asc file in the Additional Decryption Key (ADK) Path field, and enter the passphrase protecting the file,

PGP Decryption using the Passphrase

1. Enter the passphrase in the Passphrase field.



2. Click **OK**.

Dell Data Protection Enterprise (formerly Credant Mobile Guardian) Encryption Support

EnCase Forensic provides a way to decrypt files encrypted with Dell Data Protection Enterprise (formerly Credant Mobile Guardian) on Windows devices.

Enabling an Examiner Machine to Identify and Decrypt Credant Files

EnCase Forensic requires Credant DLLs in order to identify and decrypt files encrypted with Dell Data Protection Enterprise/Credant Mobile Guardian.

To enable EnCase Forensic to identify and decrypt Dell Data Protection Enterprise/Credant Mobile Guardian files:

1. Download the Credant Installer from the Guidance Software Customer Community Resource Center.
2. Run the Credant Installer on your examiner machine to create a directory structure and place the required DLLs within it. The installer also installs `CEGetBundle.exe`, which is needed for offline decryption.

There are two scenarios for decrypting files that have been encrypted with Dell Data Protection Enterprise/Credant Mobile Guardian:

- The encrypted files are accessible on the network
- The encrypted files are offline and not accessible on the network

Decrypting Credant Files Accessible on the Network

For files accessible on the network, EnCase Forensic reviews mounted volumes and searches for Dell Data Protection Enterprise/Credant Mobile Guardian encrypted files. If it finds such a file, a logon dialog displays:

1. The dialog populates with a known user name and password, Server, Machine ID, and Shield Credant ID (SCID). If the credentials are correct, Dell Data Protection Enterprise/Credant Mobile Guardian files are processed and decrypted with no further action needed.
    - If the registry file is unencrypted, then the Server, Shield CID, and Machine ID are prepopulated for the boot volume disk.
    - In an offline scenario, the **Online** checkbox is blank and the Machine ID and SCID fields are unavailable.

2. Save the case when a successful decryption is complete. The credentials entered in the dialog are stored in Secure Storage, eliminating the need to re-enter them.

Decrypting Offline Dell Data Protection Enterprise/Credant Mobile Guardian Files

If the machine to be investigated is not on the network with the Dell Data Protection Enterprise/Credant Mobile Guardian server, you must obtain the appropriate keys and store them in a location accessible to the EnCase Forensic machine.

Before you begin:

- Confirm that your EnCase Forensic license includes the EnCase Decryption Suite (EDS). EDS is included with EnCase Forensic in most countries.
- Download and run the Credant Installer on your examiner machine. You can obtain the installer from the Guidance Software Customer Community Resource Center. The installer places required Credant DLLs and the `CEGetBundle.exe` application in the EnCase Forensic \EnCase8\Lib\Credant Technologies\CMG subdirectory of your examiner machine.
- Obtain the URL for the Dell Data Protection Enterprise/Credant Mobile Guardian Device Server.
- Obtain an Administrator username and password.
    - The Dell Data Protection Enterprise/Credant Mobile Guardian administrator must have privileges specific to the version of Dell Data Protection Enterprise/Credant Mobile Guardian used with the encrypted files.

- Obtain the following:
    - Administrator's login domain (for CMG 6.0 and later servers only)
    - Machine ID for the target device (MUID)
    - Shield Credant ID (SCID)
    - Username that the key material is being downloaded for
    - Password to use to encrypt the output .bin file

To decrypt and acquire from target devices:

1. From a computer that can communicate with the Dell Data Protection Enterprise/Credant Mobile Guardian Server, run the `CEGetbundle.exe` utility from the Windows command prompt.
    - `CEGetBundle.exe` is included in the Credant Installer, which also installs the DLLs necessary for the decryption.

- Copy the integration DLLs and MAC file to the target device.
- Supply the parameters as follows: `CEGetBundle [-L] XURL -aAdminName -AAdminPwd [-DAdminDomain] [-dDuid] [-sScid] [-uUsername] -oOutputFile -oOutputFile -IOutputPwd`

-L	Legacy mode for working with pre-5.4 server installs
URL	Device Server URL (for example, https://xserver.credant.com:8081/xapi)
AdminName	Administrator user name
AdminPwd	Administrator password
AdminDomain	Administrator domain (optional: required only if the CMG Server is configured to support multiple domains)
MUID	Machine ID for the target device (also known as the Unique ID or hostname)
SCID	Shield Credant ID (also known as DCID or Device ID)
Username	Name of the forensic administrator
OutputFile	File to save the key material in
OutputPwd	Password to encrypt output file

Here is a command example: `cegetbundle -L -X"https://CredantServer:8081/xapi" -a"Administrator" -Achangeit -d"CredantWorkstation.Credant.local" -sCI7M22CU -u"Administrator" -o"C:\CredantUserKeys.bin" -iChangeIt`

2. Place the `.bin` file downloaded from the Dell Data Protection Enterprise/Credant Mobile Guardian server in a path accessible from the examiner machine. Open EnCase Forensic and create a new case or open an existing one. EnCase Decryption Suite must be installed on the Examiner machine.

   Note: In legacy mode, you must execute this utility for each user targeted for investigation on the target device while specifying the same output file. The keys for each user are appended to this output file.

3. Acquire a device with Dell Data Protection Enterprise/Credant Mobile Guardian encrypted files, or load an evidence file into the case. The Enter Credentials dialog displays,

prompting you for the username, password, server/offline server file, machine ID, and Shield Credant ID (SCID) information only.

Note: In offline mode, the only information you must provide is the password and server/offline server file (full path and filename to the `.bin` file downloaded using the `CEGetBundle.exe` utility).

When EnCase decrypts Dell Data Protection Enterprise/Credant Mobile Guardian files, the key information is placed in Secure Storage within EnCase Forensic, and saved with the case. You do not have to re-enter this information.

Decrypting Credant Files on Microsoft EFS

To decrypt a Microsoft Encrypting File System (EFS) file encrypted with Credant, you need:

- Microsoft EFS files that have already been decrypted. See Analyze EFS on page 655.
- An EnCase Forensic machine with EnCase Decryption Suite and Credant DLLs installed.
- The `CredDB.CEF` file residing in the folder. This is essential, since it contains the information to get to the decryption key.
  - If the file is encrypted, the `CredDB.CEF` stream is automatically stored with the file as metadata.
  - If the file is decrypted, the `CredDB.CEF` stream is not automatically stored, as it is not needed. This does not prevent you from storing the stream by specifically saving it to the LEF.

Note: If an encrypted file is decrypted and added, this is noted and displayed in the report.

McAfee Endpoint Encryption Support

EnCase supports McAfee Endpoint Encryption (McAfee EE) Version 7.0 for Windows and Mac. Guidance Software provides support for McAfee EE decryption for the 32 bit version only.

There are two scenarios for using McAfee EE in EnCase: Online and Offline. Both are described in the following sections.

Upon connecting, EnCase analyzes the Master Boot Record to detect the McAfee Endpoint Encryption boot signature, then displays a dialog.

ONLINE SCENARIO

Check **Online** and supply this information:

- **Username** and **Password** for EPO server admin
- **Machine Name** of the device under investigation
- EPO **Server** name
- EPO **Port** - The default for the EPO Server is 8443.

  The **Keycheck** ID is pre-populated, as read from the device. The keycheck uniquely identifies the device.

OFFLINE SCENARIO

Clear the **Online** checkbox and get the recovery file either directly from the ePolicy Orchestrator (ePO) server or by using `RequestMachineKey.exe` from a machine that can access the ePO Server.

When using the offline method, enter the recovery file in the McAfee Endpoint Encryption Recovery File field.

When using either the Online or Offline method, EnCase stores the credentials entered in the dialog in Secure Storage, eliminating the need to re-enter them.

When decryption is successful, results display in the Tree pane. Save the case.

If encryption fails, EnCase displays only the unallocated clusters.

S/MIME Encryption Support

EnCase S/MIME Encryption Support provides the ability to decrypt S/MIME-encrypted email found in PST files. Email sent or the file extensions .pst, mbox and .edb support the S/MIME PKCS #7 standard.

You must have PFX (PKCS 12 standard) certificates installed prior to parsing. PST, EDB, and MBOX mail containers are supported.

To decrypt S/MIME data:

1. Open or create a case and select **View** > **Secure Storage**.
2. Right click a folder in the left pane. A dropdown menu displays.
3. Select **Enter Items**. The Enter Items dialog displays.
4. Select the **Enter Mail Certificate** tab.

   Note: PFX is the only allowed certificate format.

5. Enter the path to the PFX certificate and the password, then click **OK**.

   The PFX certificate is decrypted and stored in Secure Storage.

EnCase performs S/MIME decryption and signature verification in the background.

The certificate is stored in Secure Storage under E-Mail Certificates folder when the proper password is entered. After you import the required certificates into Secure Storage, you can parse the email container files using the View File Structure feature in the Entry View.

When parsing is complete and successful, a directory list displays.

The **Artifacts** tab lets you view and work with content.

Troubleshooting a Failed S/MIME Decryption

If decryption fails, examine the **Artifacts** view to locate the error.

NSF Encryption Support

The Lotus Notes email client has security built in. Notes was the first widely adopted software product to use public key cryptography for client server and server server authentication and for encryption of data, and it remains the product with the largest installed base of PKI users.

The EnCase suite can decrypt encrypted Notes Storage Facility (.nsf) documents and send them to recipients within the same Domino server.

Each server user has an ID file that contains a user's:

- Encrypted private key
- Public key
- Password information
- Password recovery information

It also has an NSF file that represents the user's mailbox in 8.3 format in the default path `<domino installation folder>\data\mail\<user>.nsf`.

Recovering NSF Passwords

To retrieve the recovery password, you must have proper administrative rights on the Domino server.

1. Open the Domino Server.
2. Log on as the server administrator.

3. Click **OK**. The password ID list displays.
4. Click **OK**. The recovery password displays.
5. Click **OK**, and define users authorized to generate recovery passwords.

Lotus Notes Local Encryption Support

EnCase can decrypt a local Lotus Notes user mailbox (.nsf file suffix). The local mailbox is a replica of the corresponding encrypted mailbox on the Domino server.

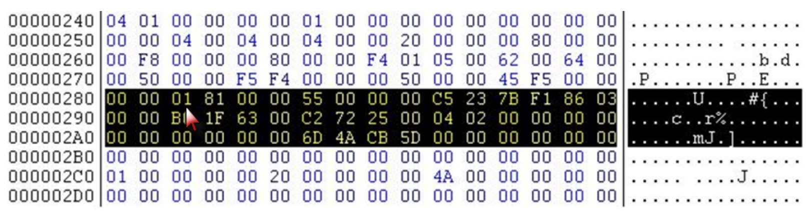
Each Domino server user has a corresponding NSF file representing that user's mailbox in 8.3 format. The default path is `<Domino Installation Folder>\Data\Mail\<user>.nsf`. The Lotus Notes client is set up to use the local mailbox. Synchronization between the local and server mailboxes occurs according to a replication schedule determined by the Domino administrator.

Encryption of the local mailbox is not mandatory but it is advisable, because without encryption a person familiar with the NSF file structure could read email without needing Lotus Notes.

Encryption occurs at block level.

Determining Local Mailbox Encryption

To determine local mailbox encryption, look in the header (the first 0x400 bytes) at offset 0x282. If the byte is 0x1, the mailbox is locally encrypted.



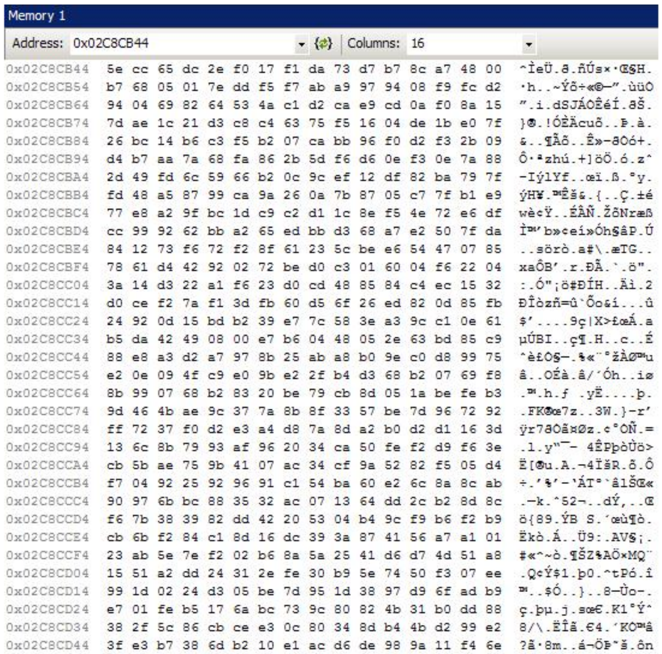
Parsing a Locally Encrypted Mailbox

To parse a locally encrypted mailbox:

1. Obtain the corresponding ID file from the Domino server. All user ID files are backed up on the server either on disk as a file or in the Domino directory as an attachment to email.
2. Parse it using **View File Structure**, so that the private key is inserted in Secure Storage.

Encrypted Block

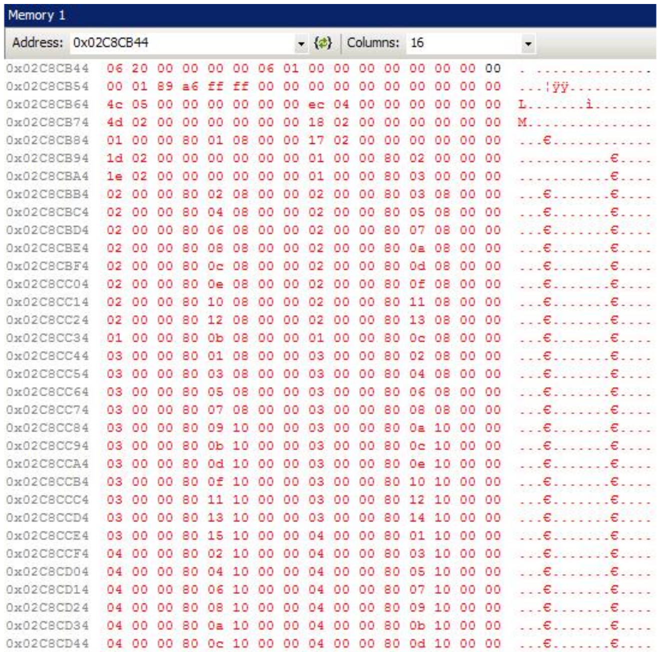
The example below shows an encrypted block at offset 0x22000:



The decryption algorithm uses a seed that is based on the basic seed from the header and the block offset.

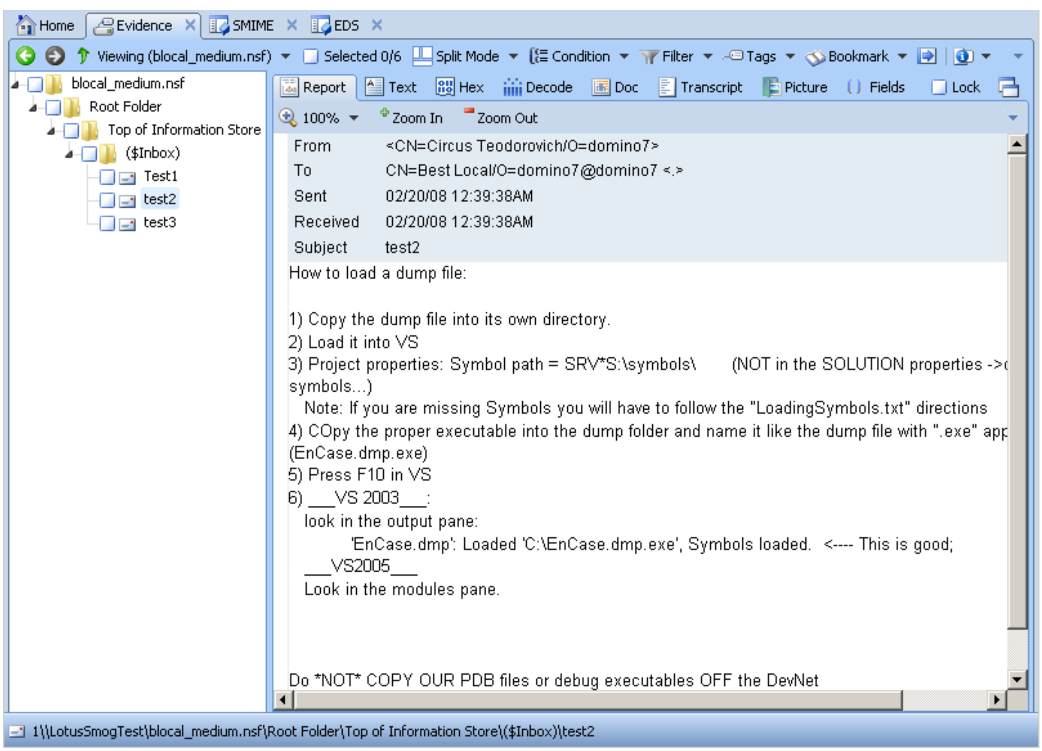
Decrypted Block

The example below shows an example of a decrypted object map at offset 0x22000:



Locally Encrypted NSF Parsing Results

Entry view displays a successfully parsed locally encrypted NSF as follows:



If the corresponding ID file cannot be parsed successfully, the Secure Storage is not populated with the data needed to parse the locally encrypted NSF; thus, the Lotus volume is empty.

Windows Rights Management Services (RMS) Support

EnCase lets you use RMS to manage decryption of Microsoft Outlook email and Microsoft Office documents across the network.

Supported products include:

- Office 2003 and 2007
- Outlook 2003, 2007, and 2010 PSTs

The two ways to decrypt RMS protected files include:

- At the volume level
- At the file level using View File Structure

For versions of Windows prior to Vista, you must install Microsoft Windows Rights Management Services Client 1.0 (SP2) before running the RMS standalone installer.

> **Note:** When decrypting RMS protected files, it is important to enter correct credentials. Since EnCase attempts to decrypt RMS protected documents even when you enter incorrect credentials, for large PST files of several GB a long wait could be a occur--up to several hours--before learning the credentials you entered did not work. So it is crucial to enter correct RMS credentials at the beginning.

RMS Decryption at the Volume Level

To decrypt RMS protected files in volume, follow these steps:

1. On the **Evidence** tab, select the volume.
2. Click the **Device** dropdown and click **Analyze RMS**.
3. The RMS credentials dialog displays.
4. Enter a Username and Password, then click **OK**.
5. EnCase decrypts RMS protected files in the volume.

EnCase stores the credentials you entered, so you do not need to enter them again.

RMS Decryption at the File Level

EnCase supports the following RMS protectors:

- MSO (Office 2003 RMS protector)
- OPC (Office 2007 RMS protector)

MSO

1. Right click the MSO protected file you want to decrypt (that is, a Word document created with Office 2003), then click **View File Structure**. The View File Structure dialog displays.
2. Select the **Find RMS Content** checkbox, then click **OK**.
3. The Microsoft RMS SuperUser Credentials dialog displays.
4. Enter a username and password, then click **OK**.
5. EnCase decrypts RMS protected files in the volume.

EnCase stores the credentials you entered, so the next time you do not need to enter them again.

OPC

1. Right click the OPC-protected file you want to decrypt (that is, a Word document created with Office 2007), then click **View File Structure**. The View File Structure dialog displays.
2. Follow steps 2 through 5 in **MSO**, above.

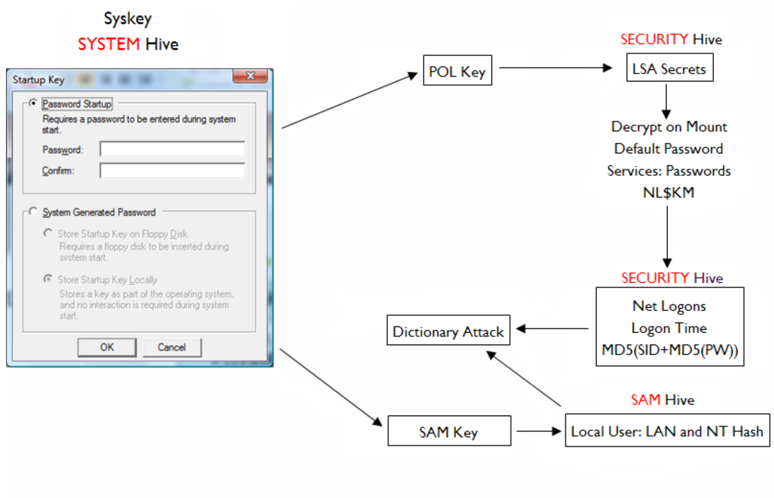
RMS Protected Email in PST

For PST files, to find email messages that are RMS protected:

1. Right click the PST file, then click **View File Structure**. The View File Structure dialog displays.
2. Select the **Find RMS Content** checkbox, then click **OK**.
3. The Microsoft RMS SuperUser Credentials dialog displays.
4. Enter a username and password, then click **OK**.

Windows Key Architecture

Windows has an elaborate key protection mechanism. The Syskey protects the policy key, the SAM key, and others. These keys protect the user's password hashes.



In Windows 2000, however, the Master Key is protected by the user's password hash with a mechanism that slows down any attack. The Master Key protects the user's private key, and the user's private key protects a key within the $EFS stream that allows for decryption of the EFS encrypted file.

Dictionary Attacks

Software implementing the dictionary attack method usually uses a text file containing a large number of passwords and phrases. Each is tried in turn in the hope that one of the words or phrases in the file will decrypt the data involved.

A large number of dictionary files (sometimes called word lists) are on the Internet, or you can create your own list. Creating your own list may be preferable if the person under investigation has particular interests that can be included in the list.

The web has freeware utilities you can use to create a dictionary from combinations of letters, numbers, and characters up to a predefined length. A search engine search for "Free Wordlist Generator" yields a number of options.

EDS can attack NT-based user account passwords and cached net logon passwords using a dictionary attack.

Built-In Attacks

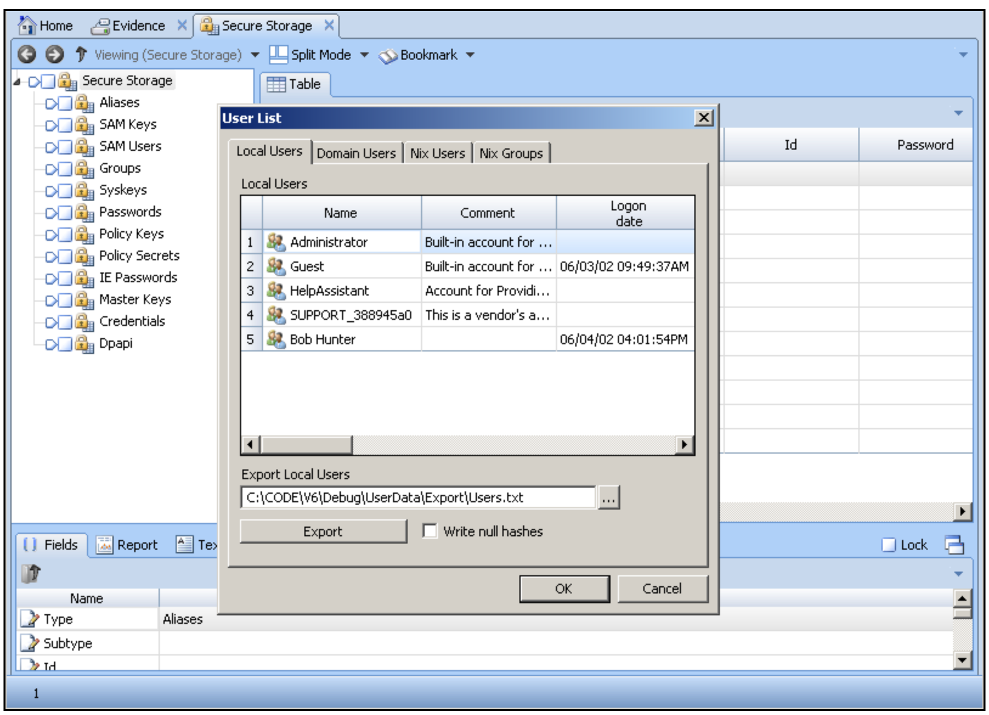
Specific items have associated passwords. If they are not automatically retrieved, you can use a trial and error mechanism.

Items that can be attacked include:

- Local users
- Network users that logged on (cached domain users)
- Syskey (password mode only)
- Master Key, if the user's SAM or domain cache can't be accessed (due to corruption, account deletion or Syskey protection). This is much slower than attacking Local/Network Users.

EXTERNAL ATTACK

Local users can be attacked with third party tools including freeware tools, whose performance is much greater than EnCase because they can run on many computers at the same time and/or use rainbow tables. EnCase can export the local user's password hashes in the PWDUMP format that most tools read. This is done from the User List:



The User List of Secure Storage displays Local Users, Domain Users, Nix Users, and/or Nix Groups from the local machine or evidence file. Information displayed includes:

- Last logon date
- User SID
- NT hash
- LanManager hash

This information is also associated with each account.

INTEGRATED ATTACK

Words to be tested may be derived from three sources:

- Internal passwords: password items in the secure storage.
- Dictionary words: the dictionary is a plain text file that can be in ANSI-Latin1 or UTF16. Every word must be on its own line (it can contain any character, including spaces).
- Brute force: automatically generates words from an alphabet with a length in a given range.

Four “mutators” can be applied:

- Toggle Case: tries all the upper/lower case variations
- Append Digits
- Prepend Digits
- Combine Words: words are combined with each other. For example, if the dictionary contains the words "old" and "dog", the result is these four words:
  - old
  - dog
  - olddog
  - dogold

BRUTE FORCE ATTACK

A brute force attack works by trying to identify a password or passphrase by testing all possible combinations of the characters of an alphabet. This alpahbet is in the text file pointed to by the "alphabet path”. This is a is a plain text file that can be in ANSI-Latin1 or UTF16, where the first line uses all the characters. This can generate very large amounts of words to test.

An example of an alphabet path is “abcdefghijklmnopqrstuvwxyz01234567890-( )“.

Depending on the settings, a dictionary attack can test thousands of passwords contained in a dictionary file in a very brief time frame. It is usual to try a dictionary attack first, then progress to a brute force attack if the password(s) cannot be found.

Any information concerning the possible structure/character length of the password helps dramatically.

CHAPTER 18

USING THE ENSCRIPT PROGRAMMING LANGUAGE

Overview 709

The EnScript Language 709

App Central 709

EnScript Launcher 709

Overview

EnScript is designed to allow a user with some knowledge of programming to access deeper functionality of EnCase Forensic, automate tasks, and create functional applications that can be shared with others.

EnScript is an object-oriented language with inheritance, virtual functions, type reflection, and a threading model.

EnScript supports COM libraries from other applications and enables you to automate document processing tasks and remote data retrieval through DCOM. You can also integrate with .NET assemblies in the form of DLL files.

The EnScript Language

The EnScript programming language has its roots in C/C++ but also contains elements of Java and C#.

It is a case-sensitive language that ignores any whitespace not part of a quoted string.

EnScript source code is processed internally as Unicode, but is stored as 8-bit text unless non-ASCII text is present.

App Central

EnScript programmers can sign up as members of the EnCase Developers Network and market their EnScript applications using EnCase App Central.

EnScript programmers signing up as an EnCase App Central EnScript developer receive the following tools:

- EnCase App Central submission tool
- EnCase App Central developer's handbook
- EnScript Fundamentals, a guide to EnScript written by the training team at Guidance Software.

EnScript Launcher

The EnScript Launcher makes it easier to locate and run EnScripts in EnCase. The launcher allows you to set up multiple EnScript databases you can search from a single, helpful menu.

When the launcher opens for the first time, you are prompted to specify up to two different file paths. You can update these paths at a later time if needed. The EnScript Launcher queries both locations for EnScripts when you search.

Once configured, the EnScript Launcher scans the provided paths recursively, keeping them up to date.

To run the EnScript Launcher:

1. In the EnScript dropdown menu, click **EnScript Launcher**, or use the keyboard shortcut **Ctrl**+**Shift**+**R**.
2. Enter the desired search term(s) and press **Tab**. Search results display in the Matching Scripts area.
3. Use the up and down arrow keys to highlight the required script, then press **Enter**.

The EnScript Launcher retains the list of paths and rescans all designated file paths whenever loaded by EnCase at startup. You can also manually edit or view your file paths via the **Edit Paths** button or rescan via the **Rescan Paths** button.

> **Note:** The EnScript Launcher does not check for duplicate script paths. Avoid entering script paths that overlap. Also, EnScripts run with the launcher do not display in the MRU list under the EnScript toolbar menu.

CHAPTER 19

VIRTUAL FILE SYSTEM

Overview	713
Evidence File Formats Supported by VFS	713
Mounting Evidence with VFS	713
Dismounting the Network Share	721
Accessing the Share	721
Third Party Tools	722
VFS Server	724
Troubleshooting the Virtual File System	728

Overview

The Virtual File System (VFS) module enables investigators to mount computer evidence as a read-only, offline network drive for examination through Windows Explorer. The feature allows investigators several examination options, including using third-party tools to examine evidence served by EnCase.

The VFS module enables the use of third-party tools against hard drives previewed through a FastBloc device or a crossover cable, including deleted files.

Evidence File Formats Supported by VFS

VFS supports mounting any data that is visible in a case. All image file formats and file systems supported by the EnCase software can be mounted with VFS.

Mounting Evidence with VFS

The VFS Module can mount computer evidence supported by EnCase as an offline, read-only network drive in Windows Explorer.

You can mount evidence at one of four levels; however, you can designate only one mounting point at a time. To change the mounting point, you need to dismount the evidence and mount at a new level to include the desired devices.

The four evidence mounting levels and associated VFS capabilities include:

- **Case level**: Mounting from case-level is not supported by VFS.
- **Disk/Device level**: Mounts a single physical disk or device, with access to all volumes on the disk or device.
- **Volume level**: Mounts a single volume/partition on a physical disk.
- **Folder level**: Mounts at the folder level, lowest level possible. This mount level is helpful to examine files in paths that exceed the Windows limit of 264 characters in the full path and name of a file.

Using the Server extension, you can also mount evidence to be shared with other investigators through a LAN. The Virtual File System Server is discussed later.

Mounting a Single Drive, Device, Volume, or Folder

Only one mount point can be designated at a time. To include other data, you must select a mount point that is in a parent relationship to both areas of data to be mounted.

To mount a single drive or device in a case file or a single volume or folder on a drive, click **Device** > **Share** > **Mount as Network Share**.

Mount Network Share Options

On the **Server Info** tab of the Mount as Network Share window, when establishing a local server, most of the server info is disabled. The only exception is the local port. VFS defaults to establishing a local server, which is the option used when using VFS on the local machine.

Since VFS is mounting the evidence as a network shared drive, a local port must be assigned. To allow recovery from errors in Windows, the VFS service runs for the life of the Windows session. This means that the port number can be assigned the first time the VFS service is run to mount evidence. Afterwards, the port number is grayed out and the assigned port number cannot be changed.

To assign a local port:

1. On the **Server Info** tab, set the local port or use the default setting.
2. Set the **Max clients allowed**, up to the maximum number of clients purchased for VFS.

   Note: The Windows session must be closed to assign a new port number.

3. Click the **Client Info** tab to set the volume letter to be assigned to the network share in Windows Explorer.
4. Windows Explorer assigns the next available volume letter by default. You can also use any other unassigned letter.

   Assigning a specific volume letter can be useful when attempting to virtually reconstruct a mapped network drive, such as for a database.

   If you currently have mapped networked drives or if you allow Windows to assign the drive letter, it takes a few seconds for Windows to query the system to find an available drive letter.

   If you specify an available volume letter, the mounting is virtually instantaneous.

A confirmation dialog informs you that the mount was successful with the volume letter. The "shared hand" icon displays at the level you designated as the mount point for the shared drive.

You can mount at the device, volume, or folder level with VFS. To do this:

1. Select the Entry you want to mount in the entry window. Click **Device** > **Share** > **Mount As Network Share**.
2. The Windows Explorer view of the mounted entry displays.

Compound Files

You can mount several different compound files, including Microsoft Word, Excel, Outlook Express, and Outlook, in the EnCase interface.

To mount a compound file:

1. Find the compound file you want to view.
2. Select **Entries** > **View File Structure**.
3. When the View File Structure operation is complete, a hyperlink displays in the entry name.
4. Click the hyperlink. The contents of the compound file display.
5. To mount the compound file, select **Device** > **Mount as Network Share**. The contents of the compound file display in Windows Explorer.

VFS displays the data.

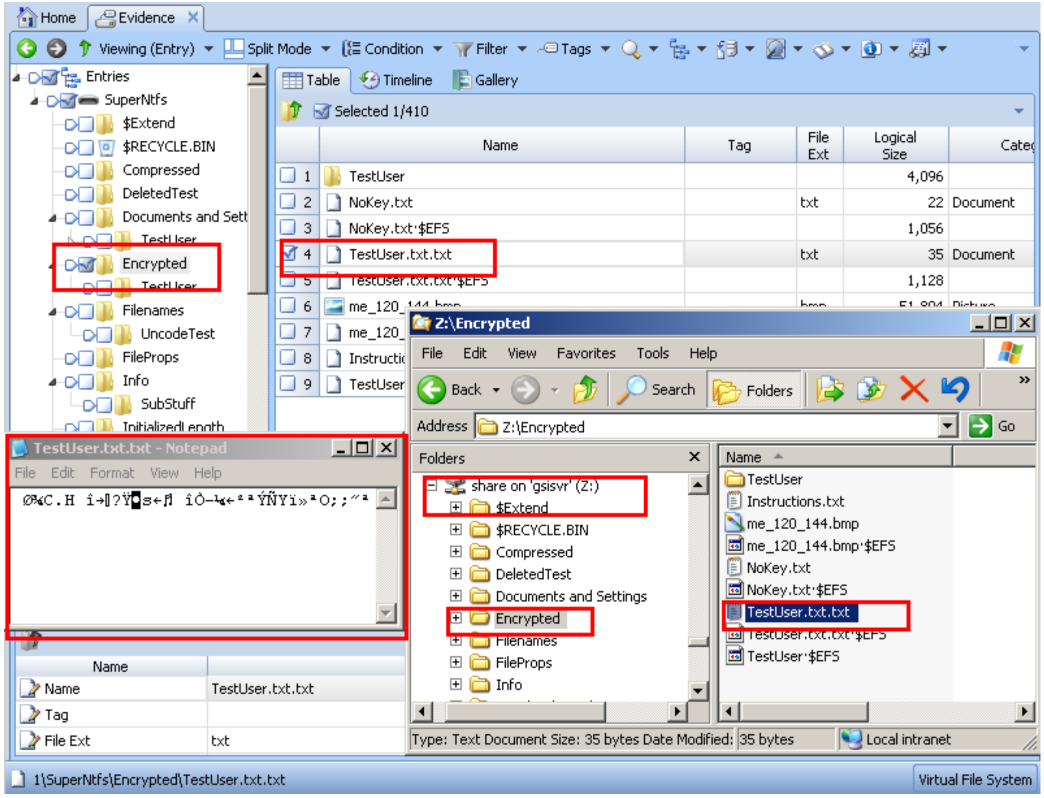
To view the original Word document file:

1. Close the mounted compound file.
2. In Windows Explorer, click **F5** to refresh the screen. If you have currently selected data within the compound file, an error message reports that the data is no longer available, since it was closed inside EnCase.
3. Select the parent folder of the file to view and open the file.

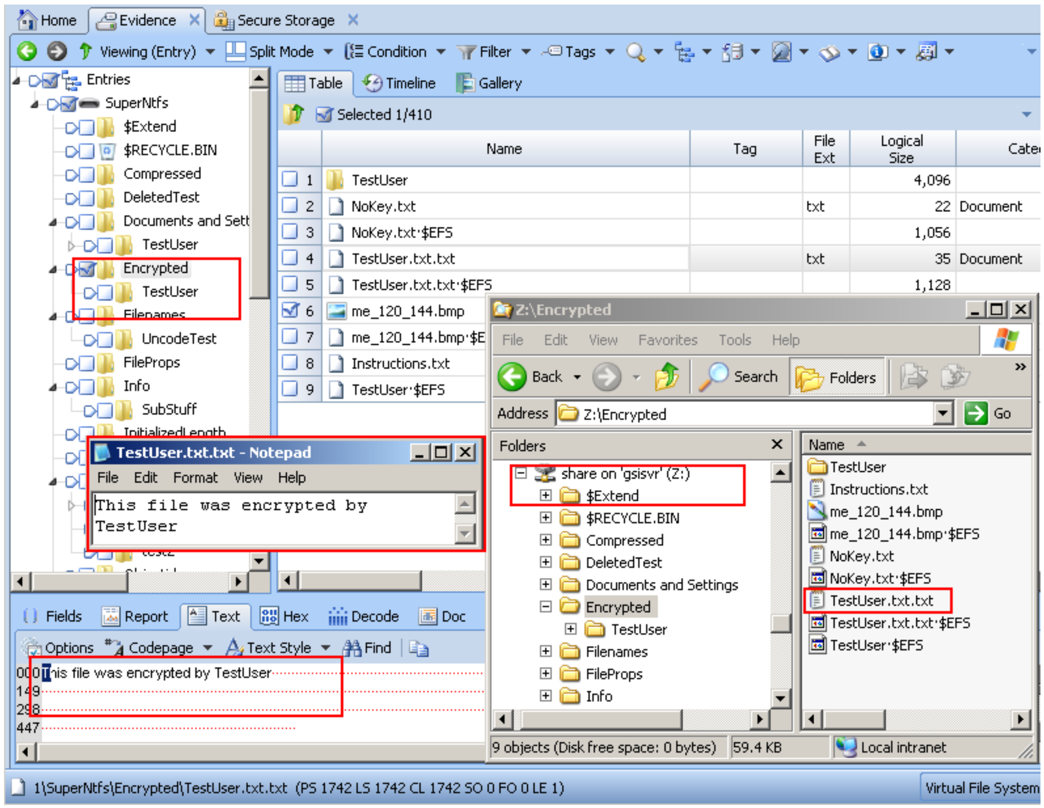
Encrypting File System

You can view decrypted files in Windows when you use VFS in conjunction with the EnCase Decryption Suite (EDS). You can mount the evidence containing the decrypted files and folders with VFS for viewing the decrypted data in Windows Explorer or with third party tools.

This is an example of an encrypted evidence file when VFS is used in conjunction with EDS:



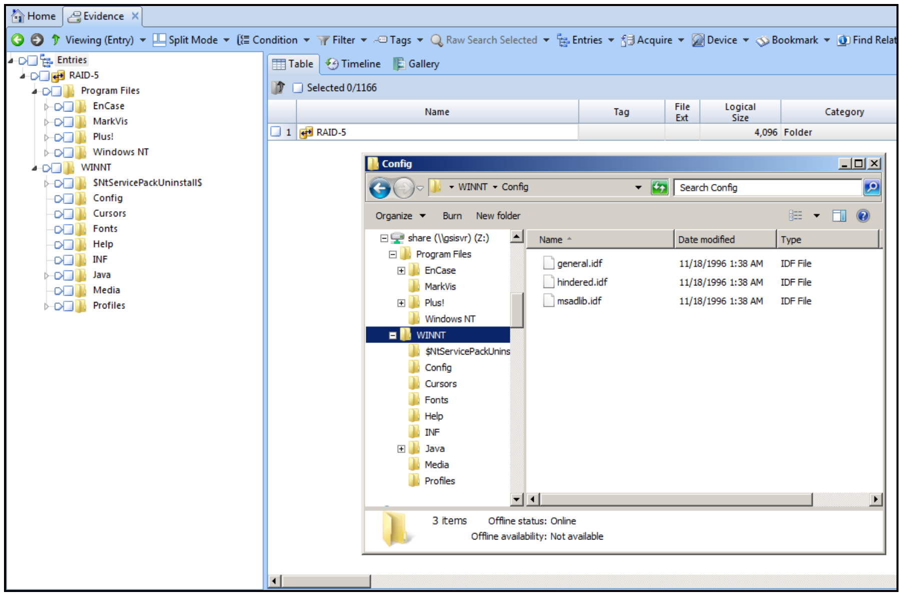
This is a view of the encrypted file in its decrypted state when using VFS in conjunction with EDS:



For more information on using EDS to decrypt EFS protected files and folders, see EnCase Decryption Suite.

RAIDs

You can browse RAIDs mounted inside EnCase in Windows Explorer. In this example, a software RAID 5 comprised of three drives was mounted, then made available for browsing in Windows Explorer with Virtual File System.



Deleted Files

The Virtual File System module lets you view deleted and overwritten files in Windows Explorer.

An investigator may locate a file in Windows Explorer to view or analyze and find that it is not possible to open the file. If a file does not open, review the original data in the EnCase interface to see if the file is valid, and is not corrupted or partially overwritten.

Internal Files and File System Files

EnCase organizes some data on devices into virtual logical files to allow for better organization and searching. Examples include unallocated clusters and volume slack on a volume, and unused disk area on a physical drive. Hidden file system files are also available, such as the $MFT, FAT, or inode table directories on NTFS, FAT, and *nix file systems.

RAM and Disk Slack

VFS serves the actual logical files on devices along with virtual logical files which it organizes for investigators. The physical files are not served, as Windows Explorer cannot interact with the file data correctly if the entire physical file was served.

For investigators, this means the RAM (sector) slack and drive (file cluster) slack are not available to third-party tools through the Virtual File System in Windows Explorer as a single file. However, you can access the data in slack with third-party tools.

To load a device without parsing the file system:

1. Launch EnCase.
2. Open a new case.
3. Click **Add evidence** > **Add Local Device**.to load the device.
4. Click **Next** to read the available local devices.
5. Clear any checkmarks from the **Read File System** column.

   When the device is loaded into EnCase, the partition and file system are not read and interpreted. You can then mount the entire device with VFS and have it be available for examination in Windows Explorer as unused disk area, including slack space.

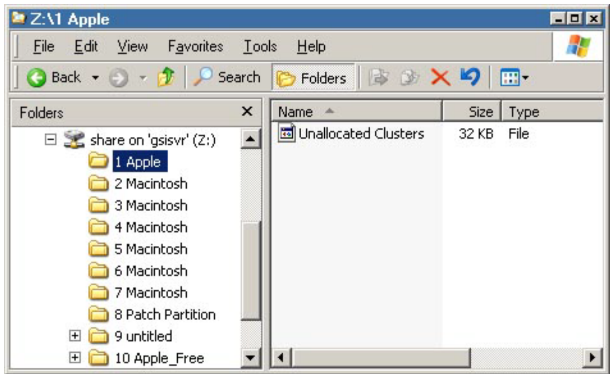
Another option is to copy only slack area from evidence to the examination computer as a logical file.

1. Select the entry with slack space to be examined.
2. Select **Entries** > **Copy Files**.
3. In the From section, select **All selected files,** and in the To section, select **Merge into one file**, then click **Next**.
4. In the **Copy** section of the Options dialog, select **RAM and Disk Slack** to copy the RAM slack (also known as sector slack) and the Disk Slack (also known as cluster slack).
5. Select the appropriate **Character Mask** option for non-ASCII characters, or accept the default and click **Next**.
6. Set the destination path and the name of the file to contain the slack and click **Finish**.
7. The progress of the copying process displays on the bottom right and the results are stored in the logs and the console.

The file containing the slack from the evidence is now available for examination by third party utilities on the local examination machine.

Other File Systems

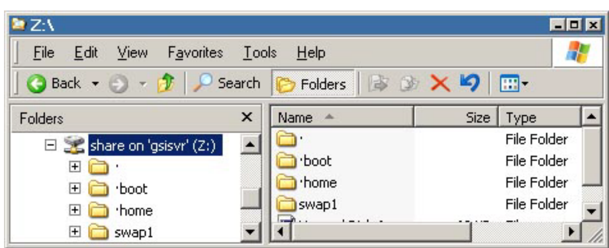
Virtual File System can mount file systems other than those natively supported by Windows. This is an example of a Macintosh OS/X drive mounted with VFS.



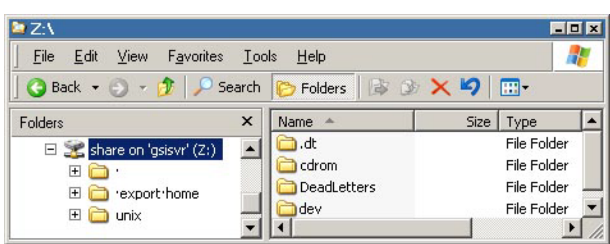
ext2, ext3, UFS, and Other File Systems

Unix, Linux, and BSD devices can be mounted in Windows Explorer with VFS. One limitation is the forward slash (/) used in *nix file systems. The forward slash is an invalid character in Windows and cannot be displayed in the full path for Windows Explorer. For this reason, the forward slash is represented by the high-dot (·).

In this example, the `/ (root)` partition is represented by the high-dot. The /home partition is represented by ·home.



In this example, the `/ (root)` partition of a Solaris workstation is mounted and the parent folder name (the partition name) displays as the high-dot.



> **Note:** Windows has a limit of 264 characters in a full path and file name. This limitation may impact some examinations in Windows Explorer, especially for Unix and Linux devices. In this situation, the investigator may need to mount at the partition or folder level.

Dismounting the Network Share

To dismount the network share:

1. Double click the **Virtual File System** thread bar at the bottom right of the screen, then click **Yes**.
2. The thread bar at the bottom right disappears, indicating the evidence was successfully dismounted.

Changing the Mount Point

You can view one mount point at a time. To change the location of the mount point, you must close the current mount point and open a new one.

> **Note:** Be sure to dismount evidence that is served through VFS before closing EnCase. A reminder message displays if you try to close the case or EnCase while evidence is mounted with VFS.

Accessing the Share

The following topics provide information about how to access and use the network share.

Using the EnCase VFS Name Column

A **VFS Name** column displays in the Table pane for the Virtual File System module. The column identifies the filename given to a file served from EnCase and displayed in Windows Explorer through VFS. The VFS name overcomes the Windows limitation of not allowing multiple files to share the same file name as siblings in the same parent folder. The column is empty when the evidence is first mounted with VFS, but populates when the share is accessed in Windows Explorer.

When an investigator selects a folder in Windows Explorer, the data is served by EnCase and displayed in Windows Explorer. As you browse directories in Windows Explorer, the file names

populate in the VFS Name column, so an investigator can determine which file is being examined. EnCase appends a pound sign (#) to the end of duplicate filenames in the same folder in Windows Explorer.

Using Windows Explorer with VFS

After mounting the shared network drive with VFS, open Windows Explorer. The new share is represented with a network drive icon and assigned the appropriate volume letter. The name of the share is gsisvr (for Guidance Software Server).

Several operations are then possible, including:

- Browsing the mounted case and associated devices in Windows Explorer.
- Opening hidden and deleted files if **Show hidden files and folders** is enabled in Windows Explorer using the **Tools** menu Folder Options.
- Using the thumbnail viewer in Windows Explorer to view images as seen by the original user.

Note: To view hidden entries, it may be necessary to update Windows Explorer settings to show all hidden files and folders.

Third Party Tools

Using Virtual File System, investigators can examine evidence outside EnCase using third party tools capable of requesting and interpreting data from Windows Explorer. However, Guidance Software does not certify the performance or accuracy of results obtained through any tools not developed by Guidance Software.

Malware Scanning with VFS

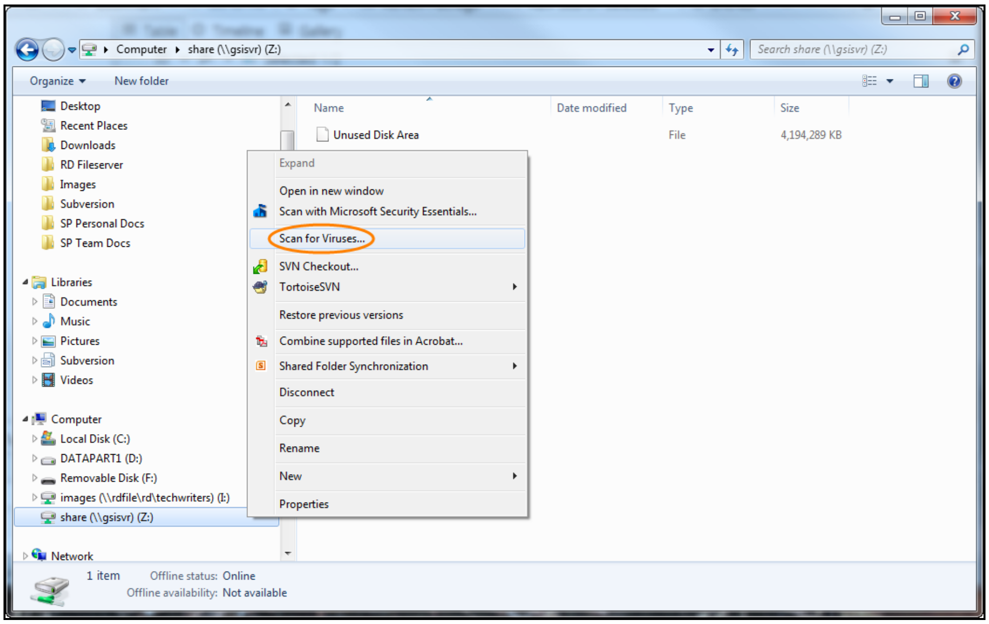
A frequent use for VFS is to mount computer evidence and scan for viruses, Trojans, and other malware programs.

1. Mount the evidence through VFS either locally on the examiner machine, or remotely through the VFS Server.

   You can mount the evidence at the device, volume, or folder levels as described previously. The "shared hand" icon indicates the level of the virtual file system mount.

2. In Windows Explorer, select the **gsisvr** offline network drive.
3. Use antivirus software to scan the file.

In the example below, the Symantec AntiVirus **Scan for Viruses** option is run by right clicking the drive.



The antivirus software can read the Virtual File System presented to Windows Explorer. The requested data is served by EnCase to Windows Explorer, then to the program for scanning.

The examination reports and logs generated by the third-party tools can be reviewed and included in the investigator's report.

Other Tools and Viewers

The third-party tools and viewers available to the investigator for forensic examination are now greatly expanded with VFS. To use them:

- Double click a file served by VFS to open the data with the program assigned according to the file extension.

ASSIGNING A FILE EXTENSION TO A PROGRAM

To associate a program with an extension:

1. From the Windows Explorer **Tools** menu, select **Folder Options**.
2. In the Folder Options window, click the **File Types** tab.

3. Select the desired extension. The Details for section lists the program designated for that extension.
4. Click **Change**.
5. Select or browse to the new program.

UNIX OR LINUX FILES

Some files, such as in Unix and Linux, do not have file extensions. To view them:

1. Right click the file and select **Open**.
2. In the Open With dialog, select the desired application from the Programs list and click **OK**.
3. If the application is not listed, click **Browse** to find the application executable, or allow Windows to search the Internet (if connected).
4. Click **Other** if the appropriate application is not available.

WordPad can open most text-based files to let you view the contents.

QUICK VIEW PLUS

Another popular viewing program, Quick View Plus, can be used to view dozens of file formats, without the native applications installed on the examination machine.

Temporary Files Reminder

EnCase allows investigators to redirect temporary files to a Temp/Trash folder on a secondary hard drive for faster cleanup after an examination, and to prevent confidential or contraband materials from being redirected by Windows to the investigator's own Temp folder on the operating system drive.

When you open a file mounted with Virtual File System in Windows Explorer with a third-party tool, the Windows operating system controls the temporary file creation on the operating system drive. Remember to check the Windows Temp folder to perform any necessary post-examination cleanup.

VFS Server

The Virtual File System module has a server extension so that investigators can share the mounted evidence with other investigators on the local area network through VFS. The extension lets clients mount the network share served by the VFS Server through a network connection, under the following conditions:

- Only the machine that is running the VFS Server needs a security key (dongle) inserted.

  A security key is not required to connect to the VFS Server and access the served data in Windows Explorer.

- The client machine(s) must have EnCase installed to access the VFS client drivers, but can run in Acquisition mode.

  The number of clients that can connect to the VFS Server depends upon the number of VFS Server connections purchased. This information is contained in the VFS Certificate or is programmed into the security key.

To determine if the VFS Server is enabled and to view the number of available client connections:

1. Select **About EnCase** from the **Help** menu.
2. If the VFS module is not listed, or if the number of clients is insufficient, contact Guidance Software Customer Service to purchase additional clients.

Configuring the VFS Server

To configure the VFS Server:

1. On the VFS Server machine (with the security key inserted), open EnCase.
2. Open the case file(s).
3. Select the appropriate VFS mount point level:
   - Case
   - Drive/device
   - Volume
   - folder
4. Right click the mount point and select **Mount as Network Share**.

   Note: You have the option of creating a network share from any of the cases, drives, or folders within it. This allows you to share only what is necessary.

5. Since this is the VFS Server machine, select **Establish local server** for the location on the **Server Info** tab.
6. Enter a Port number or use the default: 8177. The Server IP Address is grayed out since the server's IP address is the one assigned to the machine where the mount is taking place.
7. Note the server machine's IP address for use with the client.
8. Set the maximum number of clients who can connect to the server. The default is the maximum allowed by your VFS Server certificate.

Since VFS is mounting the evidence as a networked shared drive, the serving port must be assigned. To allow recovery from errors in Windows, the VFS service runs for the life of the Windows session from that port.

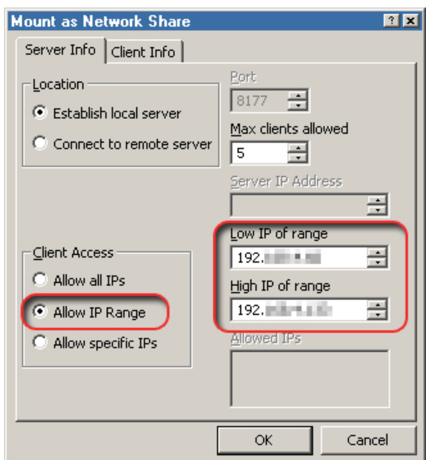
The VFS Server can also serve the data locally to the investigator's machine. It uses one of the server connections.

Restrict Access by IP Address

By default, the VFS Server is configured to allow access from all IP addresses. However, the preferred method is to restrict access by IP address.

To specify a range of machines:

1. Select **Allow IP Range** and specify the high and low IP values.



2. Select **Allow specific IPs**.
3. Right click in the Allowed IPs box.
4. Select **New** and enter the IP addresses.
5. To enter multiple IP addresses, repeat steps 3 and 4. To edit or delete existing IP addresses, right click Allowed IPs.
6. Select the **Client Info** tab.
7. To also mount and view the shared drive locally, leave the **Mount share locally** box checked and specify a volume letter.
   - By default, the volume letter field displays an asterisk, indicating that the next available drive letter will be used. Mounting the share locally uses one of your VFS Server connections.

- If you are serving the share to remote clients only, clear **Mount share locally**. The volume letter is disabled.

The VFS Server mounts the share and allows connections on the assigned port. The shared hand icon displays at the VFS mount point. You can continue your examination while it is shared. Performance depends on the size and type of the examined evidence, processing power of the server and client machines, and the bandwidth of the network.

Connecting the Clients

To connect the clients:

1. Install EnCase on the client.
2. Reboot the machine after installation for Windows to access the VFS drivers.

   When launching EnCase, it is not necessary to have a security key present.

3. Click **Tools** > **Mount as Network Share**.
4. On the **Server Info** tab, enter the Server IP Address for the VFS Server machine, and enter the port number on which the server is listening.
5. On the **Client Info** tab, select the Volume Letter to assign the share, or accept the next available letter.

A confirmation message displays.

On the client machine, the share is available in Windows Explorer as `gsisvr` with the assigned drive letter. The shared computer evidence can be examined as previously described.

Closing the Connection

When an investigator using a client machine has completed the examination of the shared drive, or another investigator needs to use the connection, double click the progress bar at the lower right and select **Yes**.

A confirmation window reports that the evidence is dismounted and the connection closed. The shared hand icon is removed, indicating that Windows Explorer has disconnected the shared drive. Close EnCase on the client computer.

On the VFS Server machine, when all clients are finished and have dismounted the share, close the VFS Server.

1. Double click the flashing **Virtual File System** bar in the lower right corner of EnCase.
2. You are prompted to dismount the evidence file. You can now close EnCase.

Troubleshooting the Virtual File System

VIRTUAL FILE SYSTEM IS NOT LISTED UNDER MODULES

If you are using cert files, check to see that the Virtual File System certificate is located in the proper Certs directory (typically `C:\Program Files\EnCase8\Certs`).

Make sure the security key is installed and working properly; check the title bar to ensure that the software is not in Acquisition mode. You do not need to have the security key installed on a machine connecting to a remote VFS Server.

If you are using cert files, the certificate file is issued for a specific security key. Check the security key ID to verify it is the correct one issued for the certificate.

A DEVICE CAN BE MOUNTED LOCALLY, BUT A LOCAL SERVER CANNOT BE SET UP

Select **About EnCase** from the **Tools** menu and ensure that Virtual File System Server is listed under Modules. If the Server is not listed, you may have the wrong cert installed, or you do not have access to the Server edition.

A CONNECTION TO A DEVICE MOUNTED ON A REMOTE VFS SERVER CANNOT BE MADE

Confirm the IP address and port number of the Remote Server. If the IP address is correct, ping the address to ensure connectivity.

Make sure the device is still mounted on the remote server.

Check to see how many machines are connected to the server, and determine how many clients are permitted to connect to a VFS Server by selecting **About EnCase** from the **Tools** menu on the machine running the VFS Server. Determine the number of allowed clients by looking at the number listed next to the Virtual File System Server module.

> **Note:** If none of these troubleshooting steps resolves your issue, contact Guidance Software Technical Services.

UNUSED DISK AREA MESSAGE

After adding evidence to a new drive on a client machine running EnCase, then running Virtual File System, when you open the new drive the new evidence is not available. Instead, the message, "Unused disk area" displays, rather than the evidence added. To correct this, on the machine where EnCase is running, configure Windows Explorer to Show hidden files, folders, and drives and to show system files.

CHAPTER 20

PHYSICAL DISK EMULATOR

Overview 731

Evidence File Formats Supported by EnCase PDE 731

Using Physical Disk Emulator 731

Third Party Tools 735

Boot Evidence Files and Live Systems with VMware 736

VMware/EnCase PDE FAQs 739

PDE Troubleshooting 740

Overview

The EnCase Physical Disk Emulator (PDE) module allows investigators to mount computer evidence as a local drive for examination through Windows Explorer. The PDE module permits investigators to employ numerous options in their examinations, including the use of third-party tools with evidence served by EnCase.

We are committed to the concept of providing an integrated product to our customers. Third-party tools continue to be developed to complement the core functions and features of EnCase, and Guidance Software encourages their creation and use. PDE allows third-party access to all supported computer evidence and file system formats. EnCase continues its evolution towards becoming a server of forensic data, whether in an image file, a preview of an offline computer or hard drive, or a live machine on a network.

Evidence File Formats Supported by EnCase PDE

EnCase PDE supports mounting individual image files of hard drives and CDs, but not images or previews of the local examiner machine's hard drive. All image file formats and file systems supported by EnCase software can be mounted with PDE.

In addition, this live computer forensic evidence is supported by PDE:

- Local machine previews of CDs.
- Local machine previews of evidence hard drives through FastBloc FE and LE hardware write blocking devices.
- Crossover cable network previews of hard drives and CDs.
- Parallel port previews of hard drives and CDs.

Using Physical Disk Emulator

Note: Do not, under any circumstances, attempt to use PDE to mount EnCase images or previews of the local forensic machine hard drives. Windows fails (displaying a blue screen) when it detects multiple instances of the same drive. Use only evidence files of other machines.

Starting Physical Disk Emulator

To mount a device using the Physical Disk Emulator module, you must add a physical or logical disk image to a case in the Entries subtab under Cases. PDE can only mount physical devices or volumes. If you select a menu item from a non-mountable level, the PDE configuration is limited to client mode.

USING PDE

1. Select the device to mount as a physical disk under Entries in the Tree pane in the **Evidence** tab and select **Device > Share > Mount as Emulated Disk**.
2. The Mount as Emulated Disk dialog displays.

Configuring the PDE Client

The Physical Disk Emulator module assigns a local port the first time you run it. Afterwards the port number is disabled and you cannot change it. To assign a new port number, close the Windows session and restart.

PDE does not use any other options in the Mount as Emulated Disk dialog **Server Info** tab.

To specify cache and CD options, click the **Client Info** tab.

CACHE OPTIONS

If you select a physical device or volume (not a CD), you can decide whether to cache data. By default, caching is disabled. Use the write cache if programs require access to the files in an emulated read/write mode.

When a cache is enabled, changes made by programs are sent to a separate cache file specified on your local system.

To create a new write cache file for an EnCase Differential Evidence File:

1. Clear the **Disable caching** checkbox.
2. Select **Create new cache** in the Cache Type box and specify a write cache path.

To use an existing write cache file, select **Use existing cache** and browse to the existing write cache file in the Write cache path field. Make sure to use a write cache file that was created with the evidence you are currently mounting.

Caching is necessary for PDE to function with VMware. In this state, Windows caches file deletions and additions. This is used to boot the drive with VMware as described later in this section. Caching is also necessary when mounting certain volume types.

CD OPTIONS

If a CD is mounted, EnCase enables the CD Session to view option, which lets you specify which session on a multi-session CD should display in Windows. The default session is the last session on the active CD, which is the one usually seen by Windows.

To view a prior session:

1. Select the **CD Session to view** option.
2. Choose a session.
3. Click **OK** to continue.
4. If a message displays stating that the software you are installing has not passed the Windows Logo test, click **Continue Anyway**.

   This lets Windows add the evidence file as a drive with its own drive letter.

   Note: If using VMware, you must have the physical device number.

Verify that the evidence file has been mounted with a drive letter by browsing in Windows Explorer. The drive letter lets you use third-party tools.

When the share is created, a sharing (hand) icon displays.

Mounting Non-Windows Devices

Devices with file systems other than NTFS, FAT, or exFAT can be mounted using the Physical Disk Emulator module, however, the volume cannot be seen by Windows (although the physical device can be seen in Disk Management). The process to mount such a device is the same as that used to mount an NTFS, FAT, or exFAT device.

Accessing the Local Disk in Windows Explorer

After mounting the disk with PDE in the EnCase interface, the new volume is represented with a hard drive icon, assigned a volume letter, and labeled as a local disk in Windows Explorer.

The mounted drive lets you:

- Open hidden files: within a Windows folder, select **Tools** > **Folder Options**. Click the **View** tab and select **Show hidden files, folders, and drives**.
- View deleted and system files and unallocated clusters.
- Mount an evidence file using the EnCase Virtual File System module.

Files and folders on the mounted device can be used in Windows in the same manner as an additional drive, although changes will be written to cache (if in use) instead of to the device itself.

Saving and Dismounting the Emulated Disk

When write caching is enabled, you can save virtual changes made to the evidence file when mounting a device.

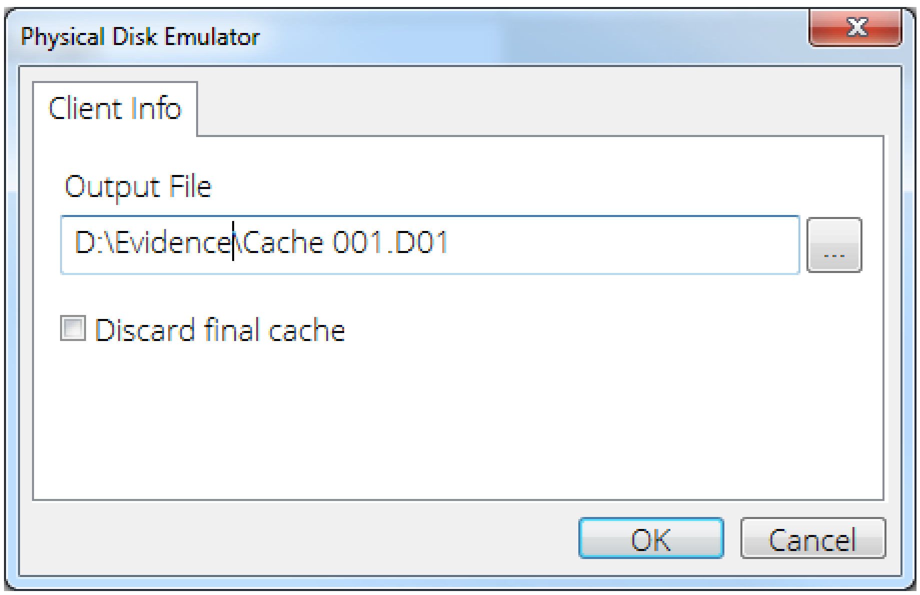
1. In EnCase, click **Device > Share > Save emulated disk state**.

EnCase saves the cache in the path specified for write caching. An instance number is appended to the cache file every time you save, after the initial save. You can later use these cache files to remount the evidence in its saved state, but you must have all of the preceding cache files located in the same directory.

To end the emulation:

1. Double click the flashing Physical Disk Emulator indicator in the lower right of the application window.
2. Click **Yes** in the Thread Status window to cancel the disk emulation.

If caching is enabled when mounting evidence, this dialog displays:



The purpose of the final cache is to create a compressed and merged Differential Evidence File (*.D01) containing the cached data. Select the **Save Emulated Disk State** option to have multiple cache files for the same mounted evidence session. The final cache merges all these files. If you do not need to save the final file, select **Discard final cache**.

Use the Differential Evidence File to open the evidence file and view the emulated disk with the cached changes applied.

To apply the cached data:

1. Right click the device.
2. Select **Mount as Emulated Disk**.
3. Click the **Client Info** tab.
4. Clear the **Disable caching** checkbox.
5. Select **Use existing cache**.
6. Browse in the Write cache path field to find the *.D01 file.

After the disk mounts, Windows Explorer reflects the cached changes.

When the device is dismounted, a status screen displays indicating the disk dismounted successfully.

Closing and Changing the Emulated Disk

To mount a different drive, first dismount the currently emulated drive as previously described. You can then set a new mount point.

> **Note:** Be sure to dismount evidence that is served through PDE before exiting. A reminder message displays if you attempt to close the case or EnCase while evidence is mounted with PDE.

Temporary Files Redirection

EnCase allows investigators to redirect temporary files to a temp or trash folder on a secondary hard drive for faster cleanup after an examination, and to prevent confidential or contraband material from being redirected by Windows to the investigator's own temp folder on the operating system drive.

When opening a file mounted with PDE in Windows Explorer with a third party tool, the Windows operating system controls the temporary file creation on the operating system drive, and any necessary post-examination cleanup is more involved.

Third Party Tools

Investigators with the Physical Disk Emulator module can use Windows Explorer to browse the structure of computer evidence. They can also use third party tools capable of requesting and interpreting data from Windows Explorer to examine evidence outside of EnCase. Guidance Software does not certify the performance of tools not developed by Guidance Software or the accuracy of their results.

Using Third Party Tools

Third party tools and viewers available to the investigator for forensic examination are greatly expanded with EnCase Physical Disk Emulator.

To use a third party tool:

1. Open the file served by PDE to have Windows Explorer request and receive the data from EnCase.
2. Open the data with the assigned program according to the file extension.

QUICK VIEW PLUS

Quick View Plus is a popular viewing program, which allows the investigator to view dozens of file formats without the native applications installed on the examination machine.

MALWARE SCANNING

A common use for EnCase PDE is to mount computer evidence for scanning for viruses, Trojans, and other malware programs.

1. Mount the drive or volume from the evidence file through PDE.
2. In Windows Explorer, select the newly mounted drive.

If an antivirus program is installed and integrated with Windows Explorer, it can scan for viruses. The program reads the emulated disk presented to Windows Explorer. EnCase serves the requested data to Windows Explorer, then to the program for scanning.

Boot Evidence Files and Live Systems with VMware

The following topics describe how to work with boot evidence files and live systems when using PDE with a VM machine.

Initial Preparation

VMware version 4.5.1, build 7568 or later is required for the Physical Disk Emulator to work properly.

To use VMware to mount an evidence file:

1. Determine the operating system of the subject evidence file:
   - Use the **Windows Initialize Case** module from the Case Processor EnScript to determine the operating system.
   - Check the contents of the boot.ini file, which is located on the partition root.
   - Examine the folder structure, noting the following:

   Windows 2000, XP, and 2003 Server all use the `C:\Documents and Settings` folder for user profiles and folders.

   Windows NT and 2000 use the `C:\WINNT` folder for the system root.

   Windows 9X, XP and 2003 Server use the `C:\Windows` folder for the system root.
2. Mount the physical disk containing the operating system using Physical Disk Emulator. Make sure to enable caching.
3. Determine the physical disk number assigned to it using one of these methods:

   This information is provided when the device is mounted.

   Select the Disk Management option: right click **My Computer** in Windows, then select **Manage**.

   Note: A problem may occur with VMware that prohibits VMware from booting a virtual machine located on a physical disk that is preceded numerically by a SCSI, FireWire, or USB drive. For best results, ensure that only IDE drives are connected to the machine when you choose to mount it as an emulated disk in the EnCase interface. This can be verified in Disk Management.

   Note: If you encounter a message stating, "The specified device is not a valid physical disk device," it is likely a result of this problem. Do not use PDE to mount drives in an evidence file or preview the local computer. Windows, particularly XP, fails (displaying a blue screen) if it detects multiple instances of the same drive. Use only evidence files of other machines.

New Virtual Machine Wizard

To boot evidence files using VMware:

1. After you have gathered the necessary information, launch VMware.
2. Select **File** > **New Virtual Machine**.
3. In the New Virtual Machine Wizard screen, click **Next**.
4. Select **Custom**, then click **Next**.
5. Select a guest operating system.
6. Select an option from the **Version** dropdown menu to identify the operating system version installed on the evidence file, then click **Next**.

7. In the Name the Virtual Machine dialog, enter a virtual machine name.
8. Click **Browse** to change the location for VMware's configuration files, if necessary.
9. Click **Next**.
10. Specify the amount of memory for VMware to use, then click **Next**.
11. Select the type of network to use, then click **Next**.

    Selecting **Do not use a network connection** is recommended when there is malware installed on the machine where the evidence file was created.

12. Click Next to accept the default setting in the Select I/O Adapter Types dialog.
13. Select **Use a physical disk (for advanced users)** and ignore any subsequent warning messages.
14. Select the disk that represents the mounted drive using PDE.
15. Accept the default setting of Use Entire Disk, then click **Next**.
16. Accept the default disk file specified in the Specify Disk File dialog, then click **Finish**.

    If the disk file is not recognized as a virtual machine, you can change the name of the file. Do not change the .vmdk extension.

    VMware returns to the main screen, displaying the newly created virtual machine.

Booting the Virtual Machine

To boot the virtual machine:

1. Start VMware.
2. Click the link for **Start this virtual machine** next to the green arrow. The evidence file is write protected by EnCase, but PDE enables a write cache that interacts with VMware as if it were mounting a disk in read/write mode. When the virtual machine starts, the operating system displays as if the forensic machine were booting the drive. It boots in the same manner as the native machine.

As with booting restored hard drives, the virtual machine may require a user name and password to proceed.

Since popups can cause driver problems, save the state of the virtual machine regularly.

VMware/EnCase PDE FAQs

CAN LIVE EVIDENCE BE BOOTED WITH VMWARE?

Live computer evidence (network nodes in EnCase Enterprise and local CDs) can be mounted with PDE but cannot be booted with VMware.

WHAT VERSION OF VMWARE SHOULD BE USED WITH ENCASE PDE?

PDE/VMware can be used with VMware version 4.5 and higher.

WHY WON'T VMWARE RECOGNIZE AN EMULATED (MOUNTED) DISK?

You must launch VMware after emulating the disk with PDE, as VMware does not recognize a physical drive added since it was started. In addition, VMware does not successfully boot evidence files which contain Windows with a non-default IDE driver. This is a known issue.

WHAT DO I DO IF I SEE THE MESSAGE "THE FILE SPECIFIED IS NOT A VIRTUAL DISK" AFTER RUNNING THE NEW VIRTUAL MACHINE WIZARD?

After completing the new virtual machine wizard in VMware, you may receive an error message ("The file specified is not a virtual disk."). This issue is with VMware. Running the new virtual machine wizard again usually resolves this issue.

HOW DO I START A VMWARE MACHINE WITH MY SAVED ENCASE DIFFERENTIAL FILE?

Mount the disk using the existing cache file.

WHY DOES VMWARE NOT RECOGNIZE SOME PHYSICAL DISKS?

If your evidence is successfully mounted, but VMware states that the physical disk the image is mounted on is not a valid physical disk, it may be a result of a non-IDE device on a physical device lower than the emulated disk.

WINDOWS KEEPS POPPING UP WINDOWS ABOUT INSTALLING DRIVERS WHEN I BOOT.

The EnCase PDE module installs GSI-specific IDE drivers which are loaded to emulate the disk as a drive in Windows with an assigned drive letter. A virtual IDE controller is created that can be seen in Device Manager. If Windows is allowed to load default IDE drivers, the module will not work properly. You can prevent this by canceling the attempt from the popup window. Once you have bypassed this message, you can save the state so the next time the system reboots, Windows does not attempt to load the drivers again.

HOW DO I RESTART A VMWARE SESSION FROM A SAVED STATE?

The VMware suspend and resume feature lets you save the current state of your virtual machine, then resume later with the virtual machine in the same state as when you stopped it. Once you resume and do additional work in the virtual machine, there is no way to return to the state the virtual machine was in when you suspended it. To preserve the state of the virtual machine so you can return to the same state repeatedly, you must take a snapshot.

Instructions for using the snapshot are on the VMware Knowledge Base at https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1009402. The speed of the suspend and resume operations depends on how much data changed while the virtual machine was running. In general, the first suspend operation takes slightly longer than later operations. When you suspend a virtual machine, it creates a file with a .vmss extension. This file contains the entire state of the virtual machine. When you resume the virtual machine, its state is restored from the .vmss file.

To suspend a virtual machine:

1. If your virtual machine is running in full screen mode, return to window mode by pressing **Ctrl + Alt**.
2. On the VMware Workstation toolbar, click **Suspend**.
3. When VMware Workstation completes the suspend operation, it is safe to exit VMware Workstation (**File** > **Exit**).

To resume a virtual machine:

1. Start VMware Workstation and choose a virtual machine you have suspended.
2. Click **Resume** on the VMware Workstation toolbar.

   Note that any applications you were running when you suspended the virtual machine are running and the content is the same as when you suspended the virtual machine.

You can obtain additional VMware troubleshooting information from their knowledge base at: https://kb.vmware.com/selfservice/microsites/microsite.do

PDE Troubleshooting

PHYSICAL DISK EMULATOR IS NOT LISTED UNDER MODULES WHEN ACCESSING ABOUT ENCASE FROM THE HELP MENU

If you are using cert files, check to see that the PDE certificate is located in the Certs directory (typically `C:\Program Files\EnCase8\Certs`).

Make sure the security key is installed and working properly (check the title bar to ensure that the program is not in Acquisition mode).

If you are using cert files, check the security key ID to verify it is the correct one issued for the certificate.

I CAN MOUNT A DEVICE LOCALLY, BUT CANNOT SET UP A LOCAL SERVER

Although menus exist for PDE Server operation, they are currently not functional.

A MESSAGE IS ENCOUNTERED STATING THAT PDE CANNOT REMOVE THE DEVICE WHEN ATTEMPTING TO DISMOUNT THE DEVICE MOUNTED

This error message may occur if Windows is accessing a file on the mounted device (for example, the directory is opened in Windows Explorer or a file is opened in a third-party application). To resolve the issue, close all Windows applications accessing the mounted device, then click **OK**.

AN ERROR MESSAGE IS ENCOUNTERED STATING THAT YOU NEED TO REBOOT YOUR MACHINE, FOLLOWED BY A "REJECTED CONNECTION" MESSAGE

This issue is due to the device driver not being released properly. The only way to resolve this issue is to close all applications (including the EnCase application) and reboot the forensic machine. You should not encounter the error again when the machine is rebooted.

Note: If these troubleshooting steps do not resolve your issue, contact Guidance Software Technical Services.

CHAPTER 21

FASTBLOC SE

Overview 745

Write Blocking and Write Protecting a Device 745

Disk Caching and Flushing the Cache 747

Troubleshooting 747

Overview

The FastBloc® SE (Software Edition) module is a collection of tools designed to control reads and writes to a drive attached to a computer through USB, FireWire, and SCSI connections. It enables the safe acquisition of subject media in Windows to an EnCase evidence file.

When the FastBloc SE module write blocking capability is enabled, it ensures that no data is written to or modified on a write blocked device.

Write Blocking and Write Protecting a Device

To write block a USB, FireWire, or SCSI device, EnCase intercepts the signal sent to Windows when a device is attached to the computer. It then filters the driver for that device, enabling write protection.

Three modes are available when using the FastBloc SE module on a USB, FireWire or SCSI device:

- **Write Blocked**: A write blocked device is protected against writing to or modifying files when the device is attached to a PC. Files deleted from or added to the device display in Windows as modified, but the modifications are saved in a local cache, not on the device itself. This mode does not display errors when attempting to write to the drive.
- **Write Protected**: A write protected device is protected against writes or modifications when the device is attached to a PC. If writes or modifications to the device are attempted, Windows displays an error message.
- **None**: Removes write blocking from a device previously write blocked.

Write Blocking a USB, FireWire, or SCSI Device

To write block a USB, FireWire, or SCSI device:

1. Make sure the subject device is not attached.
2. Click **Tools** > **FastBloc SE**.
3. In the FastBloc SE dialog, select the **Plug and Play** tab.
4. Click **Write Blocked**. The progress bar indicates EnCase is waiting for a device to be inserted.
5. Insert a USB, FireWire, or SCSI device.

    Note: Because some SCSI devices are not initially hot swappable, you may have to use a hot swappable carrier to protect the device, such as the StarTech DRW150SCSIBK SCSI drive bay.

6. Click **Close**.

Verify Write Block

To confirm successful write blocking of the device when previewing the device in EnCase:

1. Click the **New** icon on the top toolbar to open a new case and complete the required information.
2. Click the **Add Device** icon.
3. Blue check **Local Drives** in the right pane, then click **Next**.

   In the **Choose Devices** window, on the write blocked channel, the device and volume (if present) each have a green box around their icons in the **Name** column, and a bullet displays in the **Write Blocked** column for each.

Write Protecting a USB, FireWire, or SCSI Device

To write protect a USB, FireWire, or SCSI device:

1. Make sure the subject device is not attached.
2. Click **Tools** > **FastBloc SE**.
3. In the FastBloc SE dialog, select the **Plug and Play** tab.
4. Click **Write Protected**. The progress bar indicates EnCase is waiting for a device to be inserted.
5. Insert a USB, FireWire, or SCSI device.

   Note: Because some SCSI devices are not initially hot swappable, you may have to use a hot swappable carrier to protect the device, such as the StarTech DRW150SCSIBK SCSI drive bay.

6. Click **Close**.

Removing Write Block from a USB, FireWire, or SCSI Device

To remove a USB, FireWire or SCSI device:

1. Select the **Safely Remove Hardware** icon in the System Tray in the lower right corner of the task bar. In Windows 7 and Windows 8, the icon is labeled **Safely Remove Hardware and Eject Media**.
2. Remove the device physically when the wizard confirms safe removal.

Removing Write Block from one Device

1. Click **Tools** > **FastBloc SE**.
2. Select the device where you want to remove write block, then click **None**.
3. Click **Close** to complete the process.

Removing Write Block from all Devices

1. In the FastBloc SE dialog, click **Clear All**.
2. Click **Close**.

Disk Caching and Flushing the Cache

To flush the write cache, reboot the computer or remove the write blocked media. Preview the drive with EnCase or browse using Windows Explorer to verify that the cache is empty.

Troubleshooting

THE WRITE BLOCK OPTION DOES NOT DISPLAY IN THE TOOLS MENU

Check that the security key is in the machine. If the security key is missing or not functioning properly, EnCase opens in Acquisition mode.

WINDOWS AND ENCASE DO NOT RECOGNIZE THE ATTACHED DEVICE

Check all power and data connections to the device.

Check to see if the subject hard drive is spinning. If the device is connected via an external drive bay, shut down the computer and try connecting the power connector (not the data connector) to a Molex® power cable directly from the computer. Restart the computer. If the drive starts spinning, shut down the computer again and swap cables.

If the subject drive does not spin, or is making unusual sounds (whirring, clicking, etc.), the drive may be defective and you may be unable to acquire it by usual methods.

If the subject drive is spinning, check the data cables. If you are using an 80-wire cable, try using a 40-wire cable.

Check the USB or FireWire port to ensure proper functioning. Insert a known good device. Make sure the port is recognized in Device Manager.

WINDOWS SEES THE SUBJECT DRIVE, BUT ENCASE DOES NOT

If you can see the physical drive but cannot see the contents of the drive, EnCase may be in Acquisition mode. This may indicate that the security key is not installed.

You may have a corrupt version of EnCase. Uninstall EnCase, then download and reinstall the latest version.

Try to acquire on a different machine. This helps pinpoint the problem, as it may be a hardware or operating system conflict.

ACQUISITION TAKES TOO LONG

If the acquisition started at a normal speed, then rapidly decreased later in the acquisition, EnCase probably encountered bad sectors on the subject drive. Because the software makes multiple attempts at reading bad sectors, acquisition time may increase.

Enabling compression dramatically increases acquisition time.

A slow acquisition may be the result of slow equipment.

If you are acquiring to external media (that is, the storage media is an external hard drive) transfer rates are significantly slower than with a directly connected hard drive.

If the subject drive is an old or slow model, acquisition speed is limited.

If the forensic machine has an old or slow storage drive, the acquisition is limited by the drive's write speed.

If you are acquiring a newer drive, an 80-wire cable allows faster throughput. Ensure the FireWire/USB cable is securely connected at both ends.

If FireWire is not available, use a USB 2.0 connection (USB 2.0 is up to 40 times faster than USB 1.0). In addition, when using USB, limit any other CPU-intensive tasks during the acquisition, since these contribute to a loss of transfer speed.

Use FireWire ports whenever possible, since the interface is faster than USB.

ACQUISITION AND VERIFICATION HASHES DO NOT MATCH

The data integrity of the cable may be an issue. If you are using an 80-wire cable, try using a 40-wire cable, a shorter IDE cable, and/or a shielded IDE cable.

Try using a different USB or FireWire cable.

THERE ARE DIFFERENT HASH VALUES EACH TIME THE DRIVE IS HASHED

This indicates a failing drive. Because the number of sector errors increases each time, hash values change. Since the first acquisition typically contains the least number of bad sectors, use the file from that acquisition for analysis.

THERE ARE MULTIPLE BAD SECTORS AFTER ACQUISITION

This can indicate a defective drive. Ensure that the cables are securely connected to the controller and the drive.

If the subject drive is in an enclosure when you try to acquire it, it may become hot during the acquisition. Try removing the drive from the enclosure to keep it cooler. This may reduce the number of sector errors.

CHAPTER 22

SUPPORT

Overview	753
Find Support Online	753
Contact Guidance Software	756
Contact EnCase eDiscovery Review Technical Support	757

Overview

Guidance Software is committed to providing our customers with the best user experience possible. There are a variety of ways for you to get the help you need, when you need it.

This section provides information on our various support resources.

- Technical Support
- Customer Service
- Sales

Find Support Online

Guidance Software provides an array of resources to help you find answers to your questions online.

To access online support, navigate to www.guidancesoftware.com and click **Support**.

TECHNICAL SUPPORT

Links under Technical Support enable you to:

- Find contact hours, phone numbers, and hours of availability
- Browse FAQs
- Call a technical support agent
- Register your product to receive future downloads
- Access customer community forums
- Join the customer community where you can:
  - Access forums
  - Read knowledge base articles
  - Log and track issues
  - Chat with a representative
  - Download documentation
  - Download products
- Register your account

CUSTOMER SERVICE

Links under Customer Service enable you to:

- Find contact hours, phone numbers, and hours of availability
- Browse FAQs
- Call a technical support agent
- Register your product to receive future downloads
- Receive help immediately in the event of a breach
- Access customer community forums
- Join the customer community where you can:
    - Access forums
    - Read knowledge base articles
    - Log and track issues
    - Chat with a representative
    - Download documentation
    - Download products
- Register your account

SALES

Links under Sales enable you to:

- Contact sales by phone or form submission
- Request a demo
- Call a sales representative
- Request a quote
- Locate your nearest reseller

Access the Customer Community

The customer community is an online meeting place where you can:

- Register your product
- Access forums
- Read knowledge base articles
- Log and track issues
- Chat with a representative
- Download documentation
- Download products

To access the customer community navigate to https://guidance.force.com/CustomerCommunity.

Browse the Knowledge Base

The knowledge base consists of articles on a variety of topics about Guidance Software products.

The knowledge base is part of the Customer Community and may be accessed by navigating to https://guidance.force.com/CustomerCommunity.

Log and Track Issues

You can create a new support case to log issues, track existing cases, or request a new feature through the customer community at https://guidance.force.com/CustomerCommunity.

Register your Product

Register your Guidance Software product to receive product updates.

To register your product, navigate to www.guidancesoftware.com/register.

If you have trouble registering your product, contact Customer Service.

If you have trouble downloading updates after registering, contact Technical Support.

Register your Account

Registered owners of Guidance Software products gain access to the forums, knowledge base articles, and other support resources contained within the Customer Community.

To register your account, navigate to www.guidancesoftware.com and click **Support** > **Technical Support** > **Register Product**. A registration form displays.

Provide all requested information. This helps us identify you as a registered owner of a Guidance Software product.

After you complete the registration form, click **Register**.

After submitting your form, you will receive an email. Once you have verified your email address, your account will be reviewed and approved within 24 business hours.

Once your registration is approved, you can access the Customer Community by navigating to www.guidancesoftware.com and clicking **Support** > **Technical Support** > **Customer Community**.

Contact Guidance Software

There are many ways to contact Guidance Software if you want help, more information, or to provide feedback.

- Contact Sales
- Contact Customer Service
- Contact Technical Support

Contact Sales

BY TELEPHONE:

626-229-9191
888-999-9712

BY ONLINE REQUEST:

Navigate to www.guidancesoftware.com and click **Support** > **Sales** to request a demo, speak to a member of our sales team, or request a quote.

Contact Customer Service

BY TELEPHONE:

626-463-7964 (Monday through Friday, 7 am to 5 pm, Pacific Time)
866-229-9199

BY ONLINE REQUEST:

Navigate to www.guidancesoftware.com and click **Support** > **Customer Service** > **Contact**.

Contact Technical Support

Guidance Software provides telephone technical support 24 hours a day, excluding weekends and holidays, through the regional support numbers listed below. All technical support inquiries are automatically routed to either our US or UK office, depending on the time of day.

UNITED STATES:

Phone: +1 (866) 973-6577 or (626) 229-9191
Fax: +1 (626) 229-9199
1055 E. Colorado Blvd.
Pasadena, CA 91106

UNITED KINGDOM:

Phone: +44 (0) 1753-552252, Option 4
Fax: +44 (0) 1753-552232
Thames Central, 5th Floor
Hatfield Road
Slough, Berkshire UK SL1 1QE

EMEA AND APAC:

+800-4843-2623

For customers in the following countries, use your country's local exit code and call: +800-GUIDANCE (4843-2623). Do not dial US country code 1.

- Australia
- Belgium
- China-North
- China-South
- Denmark
- Finland
- France
- Germany
- Hong Kong
- Italy
- Japan
- Malaysia
- Netherlands
- New Zealand
- Norway
- Poland
- Singapore
- South Korea
- Spain
- Sweden

If you do not know your exit code, refer to http://www.howtocallabroad.com/codes.html. Dial your country's exit code, then dial 800-4843-2623.

Contact EnCase eDiscovery Review Technical Support

EnCase eDiscovery Review Technical Support representatives are available seven days a week to assist you with EnCase eDiscovery Review. You can submit questions via telephone, by email, or from within EnCase eDiscovery Review.

TELEPHONE:

866-973-6577, Option 3
Technical Support business hours are 5 AM-5 PM. Pacific Time, Monday through Friday. Calls after hours are routed to the on-call technician on duty.

EMAIL:

You can also submit Technical Support requests by email to support@encasereview.com.

ONLINE:

Click **Support** at the top right of the EnCase eDiscovery Review application window. A form displays enabling you to send a support request, report a problem, or make a suggestion. Fill in the form fields and click **Send Email** to close and submit the support request.

INDEX

A

A Device Can Be Mounted Locally, But a Local Server Cannot Be Set Up 728

Access the Customer Community 754

Accessing the Local Disk in Windows Explorer 733

Accessing the Share 721

Acquired Data 443

Acquired Data - Memory Cards 590

Acquired Data - Alcatel 548

Acquired Data - Android 470

Acquired Data - BlackBerry 489

Acquired Data - CDMA Devices 549

Acquired Data - iPod 464

Acquired Data - Kyocera CDMA 549

Acquired Data - LG 482

Acquired Data - LG CDMA 549

Acquired Data - LG GSM 552

Acquired Data - Mass Storage 592

Acquired Data - Motorola 555

Acquired Data - Nokia GSM 561

Acquired Data - Nokia Symbian 509

Acquired Data - Palm OS 518

Acquired Data - Portable Devices 590

Acquired Data - Psion 515

Acquired Data - Samsung 484

Acquired Data - Samsung CDMA 568

Acquired Data - Sanyo CDMA 575

Acquired Data - SIM Cards 584

Acquired Data - Sony Ericsson 580

Acquired Data - Symbian 6.1 492-493

Acquired Data - Symbian 7.x - 8.x 494

Acquired Data - Symbian 9.x 501

Acquired Data - Tizen 487

Acquired Data - Tom Tom GPS 544

Acquired Data - Web OS 512
Acquired Data - ZTE 583
Acquiring a Device 628
Acquiring a Disk Running in Direct ATA Mode 109
Acquiring a DriveSpace Volume 116
Acquiring a Local Drive 106
Acquiring and Processing Live Previews 191
Acquiring Data from a WebOS Based Device 510
Acquiring Data from Android OS Devices 465
Acquiring Data from Different Devices 434
Acquiring Data from GPS Devices 534
Acquiring Data from iPhones/iPods/iPads/iPod Touches 439
Acquiring Data from Memory Cards/Mass Storages/e-Readers/Portable Devices 589
Acquiring Data from PDAs 513
Acquiring Data from RIM BlackBerry Devices 488
Acquiring Data from SIM Cards 584
Acquiring Data from Symbian OS Smartphones 491
Acquiring Data from Tizen Devices 486
Acquiring Device Configuration Overlays (DCO) and Host Protected Areas (HPA) 107
Acquiring Devices and Evidence 101
Acquiring Disk Configurations 110
Acquiring in Windows using FastBloc SE 109
Acquiring in Windows without a Tableau or FastBloc Write Blocker 109
Acquiring Mobile Data 431
Acquiring Mobile Device Data (General Process Description) 435
Acquiring Non-local Drives 107
Acquiring Other Types of Supported Evidence Files 115
Acquisition 352
Acquisition via Automatic Device Detection 437
Acquisition via Manual Plug-in Selection 438

Activating an Electronic License 35
Adding a Direct Network Preview Device 131
Adding a Hyperlink to a URL 427
Adding a Job to the Portable Device 330
Adding a Local Machine to the Processor Node List 167
Adding a New Keyword 145
Adding a Remote Processor to the Processor Node List 168
Adding an External File Viewer 203
Adding and Modifying File Signature Associations 265
Adding and Removing Devices 627
Adding Constraints to Analysis Data 368
Adding Evidence by Dragging and Dropping Container Files to an Open Case 236
Adding Evidence to a Case 82
Adding Hash Libraries to a Case 288
Adding Hash Values to a Hash Set 284
Adding Images to Reports 369
Adding Processor Nodes to the Processor Manager 167
Adding Raw Image Files 117
Adding Results to a Hash Library 286
Advanced Android LG Devices FAQ 482
Agere 575
Agere Devices Physical Acquisition 572
Alias 198, 265
Analyze EFS 655
Analyzing and Reporting on Data 365
Analyzing and Tagging a Review Package 274
Analyzing File Signatures 138
Analyzing Hashes 136
Analyzing Individual Search Results 262
Analyzing Protected Files 135
Android Device Rooting 466
Android OS Devices 467
Android OS Devices FAQ 480
Android Spreadtrum Devices 485
Application Folder 47
Assigning a Unicode Font 613
Associate Selected 658

Associating File Types with a File Viewer 205
Automatic Backup 93

B

Backing up a New Case 93
Basic Report Section Editing and Formatting 406
BitLocker Encryption Support (Volume Encryption) 667
Bluetooth Connection Settings 508
Body Text Tab 404
Bookmarking Case Analyzer Data 302
Bookmarking Data for Reports 389
Bookmarking Items 295
Bookmarking Keyword Search Results 262
Bookmarking Pictures in Gallery View 306
Bookmarking Template Folders 307
Boot Evidence Files and Live Systems with VMware 736
Booting the Virtual Machine 738
Browsing and Viewing Evidence 193
Browsing Images 226
Browsing Through Evidence 223
Built-In Attacks 703

C

Canceling an Acquisition 104
Carving Images with File Carver 155
Case Backup 48, 89
Case Backup Dashboard 91
Case Folder 48
Case Operations 85
Case Options Settings 80
Case Page 166
Case Portability 87
Case Selections 85
Case Templates 81
CD-DVD Inspector File Support 115
Challenge-Response Authentication 665
Changing Case Backup Settings 95
Changing Categories and Tags for Multiple Hash Sets 290
Changing Evidence Cache Location 214
Changing Text Color 209

Changing Text Styles 204
Changing the Default Code Page 612
Changing the Evidence Path if the Evidence File is Moved 86
Changing the Mount Point 721
Changing the Tag Order 322
Check for Evidence when Loading a Case 223
Check Point Full Disk Encryption Support (Volume Encryption) 663
Checking Evidence Processor Settings and Jobs 168
Checking the Windows Application Log 55
Clean List 177
Closing and Changing the Emulated Disk 735
Closing the Connection 727
Cloud Data Importing FAQ 602
Collecting Evidence 355
Collecting Evidence from Triaged Results 364
Collection Modules 351
Color Options 42
Columns in Search Results and Bookmark Views 201
COM Port Connection Settings 507
Completing the Challenge/Response Session 684
Compound Files 715
Conditions 218
Conducting a Network Preview without a SAFE 129
Conexant 574
Conexant Physical Acquisition 571
Configuration Options 37
Configuring a Windows Override Path 49
Configuring EnCase Portable for NAS Licensing 378
Configuring EnCase to Display Non-English Characters 611
Configuring Paper Layout 399
Configuring Passware as a Viewer 660
Configuring Processor Nodes 168
Configuring the Keyboard for Additional Languages 615
Configuring the PDE Client 732
Configuring the VFS Server 725

Configuring Time Zone Settings 46
Configuring Windows for Non-English Language 615
Configuring Your Linux Distribution 622
Connecting Bookmark Folders and Report Sections 420
Connecting the Clients 727
Connection Settings - Psion 16/32-bit devices 513
Connection to Device Mounted on Remote VFS Server Cannot Be Made 728
Console Window 636
Contact Customer Service 756
Contact Guidance Software 756
Contact Sales 756
Contact Technical Support 756
Contacting EnCase eDiscovery Review Technical Support 757
Copying Evidence 365
Copying Files 269
Copying Folders 271
Creating a Custom Backup 94
Creating a Filter 216
Creating a Hash Library 282
Creating a Hash Set 283
Creating a LEF from Search Results 264
Creating a LinEn Boot Disk 621
Creating a New Condition 219
Creating a New Electronic Request File 35
Creating a New Keyword List 147
Creating a Portable Job 327
Creating a Report 366
Creating a Result Set in Entries View 163
Creating a Result Set in Records View 164
Creating a Review Package 273
Creating a Scheduled Backup 94
Creating an Index 148
Creating Custom File Types 227
Creating Direct Agents 129
Creating EnCase Portable Jobs 326
Creating Hyperlinks to an Exported Item from Report Templates 424
Creating Jobs 327
Creating New Bookmark Folders 308

Creating Result Sets in Entries and Records Views 163
Creating Tags 317
Creating Thumbnails 153
Credant Mobile Guardian Encryption Support 691
Crossover Cable Preview or Acquisition 645
Crossover Previews 192
Customizing Headers and Footers 400

D

Data Acquisition - Alcatel 548
Data Acquisition - Android 469
Data Acquisition - BlackBerry 488
Data Acquisition - CDMA Devices 548
Data Acquisition - Garmin GPS 534
Data Acquisition - iPod 464
Data Acquisition - Kyocera CDMA 549
Data Acquisition - LG 481
Data Acquisition - LG CDMA 549
Data Acquisition - LG GSM 552
Data Acquisition - Mass Storage 591
Data Acquisition - Memory Cards 590
Data Acquisition - Motorola 555
Data Acquisition - Motorola iDEN 559
Data Acquisition - Nokia GSM 561
Data Acquisition - Nokia Symbian 509
Data Acquisition - Palm OS 517
Data Acquisition - Portable Devices 590
Data Acquisition - Psion 514
Data Acquisition - Samsung 483
Data Acquisition - Samsung CDMA 568
Data Acquisition - Sanyo CDMA 575
Data Acquisition - SIM Cards 584
Data Acquisition - Sony Ericsson 580
Data Acquisition - Spreadtrum 485
Data Acquisition - Symbian 6.0 491
Data Acquisition - Symbian 6.1 492
Data Acquisition - Symbian 7.x - 8.x 494
Data Acquisition - Symbian 9.x 501
Data Acquisition - Tizen 487
Data Acquisition - Tom Tom GPS 544

Data Acquisition - WebOS 512
Data Acquisition - Windows Mobile 521
Data Acquisition - ZTE 583
Data Parsing 434
Data Paths Options 43
Data Structure Bookmarks 299
Date Options 39
Debug Options 44
Decoding Data 310
Decrypted Block 698
Decrypting a BitLocker Encrypted Device Using Recovery Key 668
Decrypting a BitLocker Encrypted Device Using Recovery Password 670
Decrypting a Disk 682
Decrypting Credant Files Accessible on the Network 691
Decrypting Credant Files on Microsoft EFS 694
Decrypting Offline Dell Data Protection Enterprise/Credant Mobile Guardian Files 692
Decrypting Sophos SGN-Encrypted Evidence Using a Challenge/Response Session in EnCase 682
Deleted Files 718
Deleting a Backup 95
Deleting a Filter 217
Deleting All Jobs from the Portable Device 333
Deleting Bookmark Folders 309
Deleting Jobs 333
Deleting Processor Nodes 170
Deleting Tags 321
Deleting Target Databases from the EnCase Portable Device 333
Dell Data Protection Enterprise Encryption Support 691
Determining Local Mailbox Encryption 697
Devices Window 627
Dictionary Attacks 702
Direct Network Previews 192
Disk and Volume Encryption 652
Disk Caching and Flushing the Cache 747
Disk Configuration Set Acquired as One Drive 113

Disk Configurations Acquired as Separate Drives 114

Dismounting the Network Share 721

Displaying Content from the Case 416

Displaying HFS+ File System Compressed Files 230

Displaying Permissions for HFS+ Files and Directories 233

Displaying Related Messages 240

DMG media file format 234

Double Files 160

Drive-to-Drive Acquisition 625

Duplicating a Job 331

Dynamic Disk 113

E

Edit Menu 638

Editing a Filter 217

Editing Bookmark Content 309

Editing Bookmark Folders 309

Editing Bookmarks 309

Editing Conditions 222

Editing Default Options 175

Editing Report Templates to Include Bookmark Folders in Reports 405

Editing the Report Template to Display Comments in Reports 410

Editing the Report Template to Include the Item Path in Reports 407

EDS Commands and Tabs 655

Enabling an Examiner Machine to Identify and Decrypt Credant Files 691

EnCase Application Folder Locations 47

EnCase Decryption Suite 649

EnCase Evidence Files 104

EnCase Forensic 23

Encrypted Block 698

Encrypting File System 715

Encrypting Media 235

Encryption 338

EnScript ii, 23, 37, 47-48, 51, 66-67, 109, 124, 148, 153, 158, 165, 182, 215, 217-218, 327, 365, 383, 397, 427-428, 612, 707, 709, 737

EnScript Application UI 165

EnScript Programming Language Overview 709

Enter Items 656

Entering Non-English Content without Using Non-English Keyboard Mapping 616

Entries View Right Click Menu 213

Evidence Cache 49

Evidence File Formats Supported by EnCase PDE 731

Evidence File Formats Supported by VFS 713

Evidence Processor Prioritization 133

Evidence Processor Settings 134

Excluded Checkbox 404

Expanding Compound Files 138

Exporting a Metadata Report to Display Hyperlinks 426

Exporting a Report 373

Exporting a Report to Display Hyperlinks 426

Exporting a Review Package 276

Exporting Data for Additional Analysis 268

Exporting Search Results for Review 272

Exporting to *.msg 241

ext2, ext3, UFS, and Other File Systems 720

Extracting Authentication Data File 599

F

FAQs 381

FastBloc SE 743

File Carver 155

File Processor 343

File Report EnScript 427

Filtering Your Evidence 215

Find Support Online 753

Finder Data and .DS_Store 232

Finding Data Using Signature Analysis 264

Finding Email 139

Finding Internet Artifacts 139

Finding Jobs 331

Finding Tagged Items 257

Finding the Location of an Evidence Item 223

Firefox Artifacts 140

Font Options 42

Force Stop 180

Formatting Report Templates 399

Full Volume Encryption (FVE) AutoUnlock Mechanism 671

G

Garmin GPS Devices FAQ 543

General Acquisition FAQ 602

Generating Reports 387

Global Application Data 50

Global Options 37

GuardianEdge Encryption Support 678

GuardianEdge Hard Disk and Symantec Endpoint Encryption Support 679

H

Hardware Disk Configuration 111

Hash 347

Hashing a Device 632

Hashing Evidence 279

Hashing Features 281

HFS+ Directories Hard Links 231

HFS+ Extended Attributes 230

Hiding Empty Report Sections 423

Hiding Tags 321

Highlighted Data or Sweeping Bookmarks 297

Hold 180

Home Page 165

Hot Keys for Tags 319

I

If EnCase Reports GuardianEdge/Symantec dlls Cannot be Opened 679

If You Already Have a Security Key 36

Imported Cloud Data 601

Importing a Review Package 276

Importing Cloud Data 598-599

Importing Data 592

Importing Data from Cellebrite UFED Casese 592

Importing Data from iOS Backup Files 593

Importing Data from RIM BlackBerry 1.x-7.x Backup Files 595

Importing Data from RIM BlackBerry 10.x Encrypted Backup Files 596

Importing GPS and KML Files 597

Importing Hash Sets 291

Importing Tarantula Data 598

Indexing Text in Slack and Unallocated Space 148

Initial Preparation 736

Inserting a Picture 403

Inserting a Table 404

Installing and Configuring EnCase 25

Installing and Configuring the Evidence Processor Node 51

Installing Drivers -Motorola 554

Installing EnCase 33

Installing the SAFE and License Manager 35

Internal Files and File System Files 718

Internet Artifacts 342

Introduction 23

iOS Logical Acquisition 440

iOS Physical Acquisition 440

iPhone Reaction during Acquisition 441

iPhone/iPad/iPod Touch FAQ 462

iPod FAQ 465

IrDA Port Connection Settings 507

J

Job Actions Menu 174

K

Keychain Parsing 161

Keyword 345

Keyword Searching Through Raw Data 257

L

Launching EnCase 77

Launching Processor Options from the Results Tab 163

LG CDMA FAQ 551

LG Devices with Android OS 4.4.2-5.1.1 480

LG GSM FAQ 553

License Manager Options 40

LinEn Command Line 640

LinEn Evidence Verification 632

LinEn Manual Page 646

LinEn Setup Under Red Hat 623

LinEn Setup Under SUSE 622

Linux Syslog Parser 158, 351

Live Previews of Local Devices 192

Load Local Device 625

Localization of Report Layout 400

Locally Encrypted NSF Parsing Results 699

Log and Track Issues 755

Log Parser Modules 349

Logical Acquisition - Garmin GPS 535

Logical Acquisition - Motorola iDEN 559

Logical Acquisition - Siemens 576-577

Logical Acquisition - Windows Mobile 522

Logical Data Acquisition - Samsung GSM 571

Logical Evidence Files 105

Logically Acquired Data - Samsung GSM 572

Lotus Notes Local Encryption Support 697

M

Macintosh Artifacts 230

Macintosh OS X Artifacts Parser 158

Macintosh OS X Media Containers 234

Maintenance 374

Malware Scanning with VFS 722

Managing Hash Sets and Hash Libraries Associated with a Case 290

McAfee Endpoint Encryption Support 694

Metadata 344

Modifying a Job 331

Modifying Report Template Formats 403

Modifying the EnCase Portable Device Configuration 375

Motorola FAQ 559

Motorola iDEN FAQ 561

Mount Network Share Options 714

Mounting a Single Drive, Device, Volume, or Folder 713

Mounting Evidence with VFS 713

Mounting Non-Windows Devices 733

Multiple Notable Files Bookmarks 301

N

Navigating the Artifacts Tab 215

Navigating the Evidence Tab 210

Navigating the Table Pane 198

Navigating the Tree Pane 197

New Virtual Machine Wizard 737

Nokia Symbian 9.x Devices FAQ 506

Nokia Symbian OS Physical Acquisition FAQ 509

Notable File Bookmarks 300

Notes Bookmarks 305

NSF Encryption Support 696

NSRL Hash Sets 291

O

Obtaining a Linux Distribution 622

Obtaining Additional Decryption Key (ADK) Information 690

Obtaining Response Codes from the Sophos SGN Website 683

Obtaining Whole Disk Recovery Token Information 689

Opening the Processor Manager 167

Other File Systems 719

Other Tools and Viewers 723

Overview 27, 77, 91, 103, 123, 195, 245, 281, 297, 317, 325, 389, 433, 611, 621, 652, 713, 731, 745, 753

Overwriting the Evidence Cache 164

P

Palm OS Devices FAQ 520

Parsing a Locally Encrypted Mailbox 697

Passware Integration 659

Pause Queue 176

PDE Troubleshooting 740

Performance Monitoring 177

Performing Acquisitions with LinEn 623

Personal Information 338

PGP Decryption using the Passphrase 690

PGP Whole Disk Encryption (WDE) Support 689

Physical Acquisition - Garmin GPS 543

Physical Acquisition - Motorola iDEN 560

Physical Acquisition - Siemens 577, 580

Physical Acquisition - Windows Mobile 533

Physical Disk Emulator 729

Physical RAID Encryption Support 672

Picture 348

Portable Device FAQ 590

Preparing Additional USB Storage Devices 377

Preparing Device for Acquisition 467

Preparing Device for Acquisition - LG 481

Preparing Device for Acquisition - Samsung 483

Preparing Device for Acquisition - Tizen 487

Preparing Device for Acquisition - WebOS 510

Preparing Environment for Acquisition - Spreadtrum 485

Preparing Portable Devices 374

Printing a Condition 222

Process Evidence Menu 170

Processing a Result Set 162

Processing Evidence 121

Processing Files Using Hash Finder 361

Processing Files Using Keyword Finder 359

Processing Files Using Metadata Entry Conditions 358

Processing Files Using Picture Finder 362

Processor Manager 166

Processor Manager Error and Information Messages 181

Processor Manager Tab 173

Processor Manager Toolbar 178

Processor Manager Trace Messages 190

Processor Node Installation 167

Psion 16/32-bit Devices FAQ 517

Q

Querying a Hash Library 287

Queue 178

Queuing Evidence for Processing 171

Quickly Viewing Decoded Data 311

R

RAID-10 111

RAIDs 717

RAM and Disk Slack 718

Raw Image Files 105

Raw Text Bookmarks 297

Reacquiring Evidence 116

Reacquiring Evidence Files 117

Reactivating an Electronic License 36

Reading the Knowledge Base 755

Recovering Folders 135

Recovering NSF Passwords 696

Recovery Key and Recovery Password Files 667

Refreshing Search Results during a Keyword Search 260

Register your Account 755

Register your Product 755

Registering your Product 27

Reinstalling EnCase 37

Removing Write Block from a USB, FireWire, or SCSI Device 746

Renaming Bookmarks 310

Repairing and Recovering Inconsistent EDB Database Files 237

Report Object Code (ROC) 413

Report Styles 400

Report Template Structure 398

Report Template Wizard 420

Reserved Characters 256

Restoring a Case from Backup 97

Restoring a Drive 118

Restrict Access by IP Address 726

Result Set Processing 162

Retaining the GUID During Evidence Reacquisition 117

Retrieving Keyword Search Results 261

Right Hamburger Menu 209

RIM BlackBerry FAQ 490

RMS Decryption at the File Level 701

RMS Decryption at the Volume Level 700

RMS Protected Email in PST 701

ROC Layout Elements 413

Running a Default Filter 216

Running a Portable Job 355

Running an Existing Condition 218

Running EnScript Modules 153

Running Evidence Processor Options Incrementally 127

Running File Carver 157

Running File Signature Analysis against Selected Files 267

Running the File Report EnScript 428

S

S/MIME Encryption Support 695

Safari Artifacts 141

Safeboot Encryption Support 660

Samsung CDMA FAQ 571

Samsung Devices with Android 4.4.4-6.0.1 FAQ 484

Samsung Devices with Android OS 4.4.4-6.0.1 483

Samsung GSM FAQ 575

Saved BitLocker Credentials in Secure Storage 675

Saving Acquisition Information 632

Saving and Dismounting the Emulated Disk 733

Saving the File Report 429

Screen Capture 354

Search Fields 255

Search Modules 338

Search Operators and Term Modifiers 249

Searching for Keywords for Process Memory 147

Searching Indexed Data 246

Searching Through Evidence 243

Searching With Keywords 143

Secure Storage - Add Local User 208

Secure Storage Items 658

Secure Storage Tab 656

Secure Storage Tab and EFS 656

Select Tagged Items 322

Selecting a Language Index 151

Selecting Target Databases 366

Selecting/Clearing All Jobs 178

Set Manager Name 176

Setting Individual Case Options 84

Setting the Date Format 613

Settings and Options 92

Setup for a Drive-to-Drive Acquisition 624

Sharing Conditions 222

Sharing Filters 217
Show Conversation 239
Show Logging 190
Showing Duplicate Email Messages in a Conversation 241
Siemens FAQ 580
Siena Series 514
SIM Card Reader FAQ 588
Single Files 106
Single Notable File Bookmarks 300
Snapshot 352
Snapshot Reports 371
Software RAID 110
Sophos SafeGuard Support 682
Source code 217, 221, 709
Sources of Acquisitions 103
Sparse Bundle 235
Sparse Image 235
Specifying a Backup Location 97
Specifying a Case File 96
Starting Physical Disk Emulator 731
Stop 180
Streamlined DMG Decryption 162
Successful BitLocker Decryption 673
Support 751
Support for EXT4 Linux Software RAID Arrays 112
Supported Cards - Memory Cards 590
Supported Encryption Products 653
Supported GuardianEdge Encryption Algorithms 678
Supported Models 459
Supported Models- Symbian 6.1 493
Supported Models - Alcatel 548
Supported Models - Android 479
Supported Models - BlackBerry 490
Supported Models - CDMA Devices 549
Supported Models - Garmin GPS 543
Supported Models - Kyocera CDMA 549
Supported Models - LG 482
Supported Models - LG CDMA 551
Supported Models - LG GSM 553
Supported Models - Motorola 559
Supported Models - Motorola iDEN 561
Supported Models - Nokia GSM 567

Supported Models - Nokia Symbian 509

Supported Models - Palm OS 520

Supported Models - Portable Devices 590

Supported Models - Samsung 484

Supported Models - Samsung CDMA 570

Supported Models - Sanyo CDMA 576

Supported Models - Sony Ericsson 583

Supported Models - Spreadtrum 486

Supported Models - Symbian 6.0 492

Supported Models - Symbian 7.x - 8.x 501

Supported Models - Symbian 9.x 506

Supported Models - Tizen 488

Supported Models - Tom Tom GPS 546

Supported Models - WebOS 512

Supported Models - Windows Mobile 533

Supported Models - ZTE 583

Supported Models (Card Readers) - SIM Cards 586

Supported Utimaco SafeGuard Easy Encryption Algorithms 685

Symantec Encryption Support 681

Symbian OS 6.1 Devices FAQ 493

Sysol 574

Sysol Devices Physical Acquisition 572

System Info Parser 154, 335

System Info Parser Live Registry Analysis 155

System Modules 334

System Requirements 27

T

Table Bookmarks 304

Tagging Items 315, 319

Temporary Files Redirection 735

Temporary Files Reminder 724

Terms and Definitions 173

Text Styles 615

The Device Window 631

The EnCase Interface 195

Third-Party Tools 722, 735
Thread Monitor Window 637
Tizen Devices FAQ 488
Transcript Bookmarks 304
Triaging Personal Information 363
Troubleshooting 379, 728, 747
Troubleshooting a Failed S/MIME Decryption 696
Types of Data Acquisition 433
Types of Evidence Files 104

U

Undocking the View Pane 207
Uninstalling EnCase 36
Unix Login 158, 350
Unsuccessful BitLocker Decryption 674
Unused Disk Area Message 728
Updating Older Jobs 332
User Application Data 49
User Data 48
Username and Password Authentication 663
Using a Case Template to Create a Case 79
Using a Write Blocker 108
Using Bookmarks to Link to an External File 424
Using Disk View to See Data on a Device 214
Using EnCase Portable 323
Using LinEn 619
Using Pathways Overview 59
Using Physical Disk Emulator 731
Using Report Templates 397
Using the EnCase VFS Name Column 721
Using the EnScript Programming Language 707
Using the License Manager 32
Using Third-Party Tools 736
Using View File Structure with Macintosh Data 236
Using Views/Tabs 208
Using Windows Explorer with VFS 722
Utimaco Challenge/Response Support 685
Utimaco SafeGuard Easy Encryption Known Limitation 688
Utimaco SafeGuard Easy Encryption Support 685

V

Verifying Evidence Files 106, 633
VFS Server 724
Viewing a Report 429
Viewing and Deleting Individual Hash Items 290
Viewing Attachments 239
Viewing Case Backup Options 94
Viewing Compound Files 236
Viewing Content in the View Pane 202
Viewing Decoded Data 206
Viewing Decoded Data by Type 311
Viewing Email 238
Viewing Evidence 227
Viewing Hash Sets Associated with an Entry 288
Viewing Information in a Timeline 200
Viewing Multiple Evidence Files Simultaneously 229
Viewing Multiple Records Simultaneously 229
Viewing Notes Bookmarks 305
Viewing Processed Evidence 236
Viewing Related Items 226
Viewing Results to Triage Information 357
Viewing Saved Search Results 262
Viewing Tagged Items 320
Viewing Unicode Files 614
Virtual File System 711
Virtual File System Is Not Listed Under Modules 728
VLSI 574
VLSI Devices Physical Acquisition 571
VMware/EnCase PDE FAQs 739

W

WebOS Devices FAQ 513
Window Menu 636
Windows-based Acquisitions with Tableau and FastBloc Write Blockers 108
Windows Artifact Parser 157, 337
Windows Event Log Parser 157, 350
Windows Key Architecture 701
Windows Mobile Devices FAQ 534

Windows NT Software Disk Configurations 111

Windows Rights Management Services (RMS) Support 700

WinMagic SecureDoc Encryption Support 675

WinMagic SecureDoc Self Encrypting Drive (SED) Support 677

Working with Bookmark Folders 307

Working with Bookmark Types 297

Working with Cases 75

Working with Columns 200

Working with Hash Libraries 282

Working with Non-English Languages 609

Write Blocking a USB, FireWire, or SCSI Device 745

Write Blocking and Write Protecting a Device 745

Write Protecting a USB, FireWire, or SCSI Device 746

X

X DateAdded 161